Security Threats and Solution in Wireless Sensor Networks

K. Nataraj

1Bharathidasan University, School of Computer Science, Engineering and Applications, Tiruchirappalli-620 023, Tamil Nadu, India

Abstract: The Wireless Sensor Network (WSN) increasingly becoming more practicable solution to many challenging applications. One of the major applications of the sensor networks is in military. So providing security is particularly challenging and its security mechanisms are also be the greatest concern to deploy sensor network such hostile unattended environments, monitoring real world applications. In this paper we attempt to analyze the various threat models, attacks on WSN and respective defensive measures available relevant to security networks highlighting their advantages and weaknesses.

Keywords: attacks, threats, security, sensor nodes, wireless sensor network

1. Introduction

Wireless Sensor Network is a promising platform for a variety of application areas in such as environmental monitoring, battlefield surveillance, and homeland security domains and it is attracting many researchers to work on various problems related to this domain. The coverage, connectivity and energy related issues are very important in WSNs. But WSNs appears that they are more prone to attacks than wired networks. In applications like military, without security, the use of Wireless Sensor Network is any application would result in disastrous consequences. Security allows Wireless Sensor Networks to be used to maintain integrity of data and availability of all messages in the presence of resourceful adversaries. The main objective of confidentiality and authenticity is expected in sensor networks to safe guard the information traveling among the nodes of the network or between the sensor nodes and the sink node from disclosure.

The WSNs are comprised of a group of nodes for scalar or multidimensional data gathering. Sensor nodes are employed to collect the information, compress and process it for storage purpose and to transmit the processed data to a sink such as an intermediate cluster head or a base station (also called as gateway sometimes). The transmitted information is then presented to the system by base station connection. They are open to different varieties of attacks, including node capture, and denial of service and tampering physically.

Promoting a range of fundamental research challenges. In WSNs, the primary challenges of sensor networks are by two facts. First, sensors are extremely energy constrained. Secondly, in most of the applications nodes will be randomly deployed. This randomness leads to the issue of dimensioning the sensor network. The nodes deployed may be either in a controlled environment where monitoring, maintenance and surveillance are very difficult. In the uncontrolled environments, security for sensor networks becomes extremely important.

2. Security Threats and Solution in Wireless Sensor Networks (WSN)

2.1 Wormhole Attacks

A devastating attack is known as the wormhole attack, where more than two malicious colluding sensor nodes does a virtual tunnel in the wireless sensor network, which is used to forward message packets between the tunnel edge points. This tunnel establishes shorter links in the network. In which adversary documents forwards packets at one location in the sensor network, tunnels them to different location, and re-forwards them into the sensor network. In sensor network when sender node sends a message to another receiver node in the network. Then the receiving node tries to send the message to its neighboring nodes. The neighbor sensor nodes assume that the message was sent by the sender node (this is normally out of range), so they tries to forward the message to the originating node, but this message never comes because it is too far away. Wormhole attack is a great threat to sensor networks since, this type of attack will not require compromising a wireless sensor in the network instead; it could be performed even at the starting phase during the sensors initializes to identify its neighboring information. This Wormhole attacks are very difficult to stop since routing information given by a sensor node is very difficult to check. The wormhole attack is possible even when the attacker has not compromised with any hosts nodes and even if all communication provides confidentiality and are authenticated.

2.1.1 Countermeasures against Wormhole attacks

In authors proposed a solution to wormhole attacks for wireless sensor adhoc networks in which all sensor nodes are equipped by directional antennas. In these method nodes utilizes predefined sectors of their antennas to communicate with one another. Each pair of sensor nodes has to check the direction of received message signals by its neighboring sensor node. Thereby, the neighbor relation is established only when the directions of both couples are matched. This additional information makes wormhole discovery and intern introduces great amount of inconsistencies in the sensor network, and this can be easily be detected.
In this presentation, each sensor node calculates the distance to its neighbors based on signal strength received. Each and every sensor informs this distance data to the central controller, which studies the sensor network’s physical topology depending upon every sensor node distance measurements. Without presence of wormholes, the sensor network topology should be almost flat, whereas a wormhole would be observed as a string stretching different ends of the wireless sensor network together. Song et al presents a wormhole discovery mechanism which is depending on statistical analysis of multipath routing. Song noted that a link established by a wormhole is attractive in routing sense, and this will be selected and requested with very high frequency as it only uses routing information which is already available to a sensor node. This information’s allow for easy integration of this type into intrusion detection methods only to routing guidelines that multipath.

2.2 Sinkhole Attack

In this case a compromised sensor node tries to influence the information to it from each and every neighboring node. Thereby, sensor node eavesdrops on each and every information being communicated with its neighboring sensor nodes.

2.2.1 Sinkhole Prevention

One motivation for a sinkhole attack is that it always makes very selective forwarding trivial. By confirming that all traffic in the selected area moves through a compromised sensor node, an adversary can selectively suppress or alter the packets moving from any sensor node in the given area. It is observed that the reason networks are susceptible to sinkhole attacks is because of their specialized communication structure. Since all packets share the same destination to influence a potentially very big number of sensor nodes a compromised node required only to give a high quality route to the base station. The proposed a genetic algorithm based method to result in an approximation to the better source- visiting method. The usage of Mobile node in computer networks has some advantages and also disadvantages, naming, code caching, safety and security which is based on the given scenario. Irrespective of, they have been properly deployed in many usage starting from e- commerce to most security expected military applications.

2.3 Sybil Attack

It is defined as a malicious device illegitimately taking on number of identities. In this Sybil attack, a single sensor node i.e. a malicious sensor device will appear to be a set of sensor devices and it will forward the incorrect message to a sensor node in the network which definitely decreases the normal performance of fault tolerant such as distributed storage, dispersity and paths. This incorrect message may be any things, which may include the position of sensor nodes, strength; the generation of node which is not actually exists.

2.3.1 Sybil prevention

Public key cryptography can also be used to prevent such an insider attack, this is very expensive and it may be used in the energy constrained wireless sensor networks. Sybil attacks can be prevented by utilizing identity certificates. It employs a simple logic, before the deployment of sensor nodes, that the server node designates unique information to each of the sensor nodes. Soon after that the server creates an identity certificate binding this node’s identity to given designated unique information, and downloads the message onto the sensor node. To securely reveal its identity, a sensor node first gives up its identity certificate information, and then proves that it matches the unique information. The whole process requires good number of exchanging of messages. Normally, Merkle hash tree can be used for computing identity certificates. This Merkle hash tree vertex-labeled binary tree, in which it has two child vertexes. The first primary path of a leaf vertex is a group of vertexes on the path from its leaf to tree’s root. The vertex, its authenticated paths, and the primary path along with hash functions can be calculated. This result is compared with the stored value, to check the authenticity of the label of leaf vertex.

2.4 Hello flood attack

In, authors introduced “Hello Flood Attack”. In this, HELLO packets will have high radio transmission range and these are used as weapons in WSN. This processing power sends HELLO packets to a number of sensor nodes which are deployed in a large area within a Wireless Sensor Network. The sensor devices are thus persuaded that the adversary is their neighboring nodes. As a result of this, while forwarding the messages to the base station, the victim sensor nodes try to go through the attacker as they are aware, that it is their neighbors and are spoofed by the attacker.

2.4.1 Countermeasures against Hello Flood Attack

To prevent the hello flood attack cryptographic technique is employed. In this type of techniques two sensors use same secret key. During the communication the new encryption key is generated. This ensures that only reachable nodes can decrypt and checks the message and thereby prevents the adversary from attacking the sensor network. The disadvantage of this technique is that any attacker can spoof its identity and then starts attacks. In author presented a data forwarding technique called Multi-path multi-base station, in which a sensor node maintains number of different secrets in a multiple tree.

Sensor device can sent to its sensed information to multiple routes by employing these keys or secrets. In these multiple base stations have control over specific number of nodes of the WSN? Each base stations share all the secrets which is there with all sensor nodes, in accordance with key assignment protocol. This process is very inefficient, since the given shared secret, developed secrete key between the nodes, route setup requires maximum processing. Given the shared secret and the generated new key between two sensor nodes, the process of route setup requires much processing hence is inefficient.

The complete comparison between Layer based treats and possible counter measure in Wireless Sensor Networks have been shown in the table 1.
## Table 1: Typical Layer based treats and possible counter measure in Wireless Sensor Networks.

<table>
<thead>
<tr>
<th>S. No</th>
<th>Layer</th>
<th>Treat</th>
<th>Counter measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Physical Layer</td>
<td>Jamming, Node Tampering and</td>
<td>Use Spread-Spectrum techniques and MAC layer admission control mechanisms, low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Eavesdropping</td>
<td>duty Cycle, Tamper-Proofing, effective key management schemes, Directional</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>antennas for access restriction &amp; To protect data confidentiality, cryptography</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>is indispensable</td>
</tr>
<tr>
<td>2</td>
<td>Data Link Layer</td>
<td>Exhausting, Collision and</td>
<td>Use Spread-Spectrum techniques &amp; Error Correcting Codes, Rate Limitation. (MAC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fairness (Adversaries can</td>
<td>Layer can exclude the attacking nodes from interactions)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>disobey the coordination rules</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>and produce malicious traffic</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>interrupt network operations</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>in the MAC layer</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Network Layer</td>
<td>Sybil Attack, Sinkhole, Wormhole</td>
<td>Authentication, Monitoring, Redundancy, Flexible Routing, monitoring two-way</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and Hello flood, Neglect &amp;</td>
<td>authentication, three-way handshake, Verification of the bidirectionality of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Greedy (tampering with routing</td>
<td>link, some countermeasures are available as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>service such as modifying</td>
<td><strong>Routing Access Restriction</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>routing information and</td>
<td><strong>False Routing Information Detection</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>replicating data packets)</td>
<td>• Wormhole Detection</td>
</tr>
<tr>
<td>4</td>
<td>Transport Layer</td>
<td>Flooding, Injects false</td>
<td>Authentication and Limiting Connection Numbers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>messages and energy drain</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>and energy drain attacks</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Application Layer</td>
<td>Attacks on reliability and</td>
<td>Unique Pair-wise keys and Cryptographic approach.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clone Attack</td>
<td>Data Integrity Protection: authentication can be used to protect any data integrity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Clock Skewing</td>
<td>Data Confidentiality Protection: Encryption is an effective approach to prevent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Selective Message Forwarding</td>
<td>attackers from understanding captured data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data Aggregation Distortion</td>
<td></td>
</tr>
</tbody>
</table>

The comparison between Class of routing protocols and possible attacks in Wireless Sensor Networks have been shown in the table 2.

## Table 2: Class of routing protocols and possible attacks

<table>
<thead>
<tr>
<th>S. No</th>
<th>Protocol</th>
<th>Sink Hole</th>
<th>Sybil</th>
<th>Wormhole</th>
<th>Hello Flood</th>
<th>Black Hole</th>
<th>Energy Drain</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Flat Based Routing Protocol</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Hierarchical</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Location-Based</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>Network Flow and QoS-aware</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### 3. Conclusion

The aim of this paper is to discuss to wireless sensor network security is vast, with various attack models and counter measures proposed by various researchers. Countermeasures for these attacks exist at different sensor network levels and they are aimed at giving protection to the data during different levels of the receiving, processing and distribution process. Various methodologies are presented for ensuring security in WSNs have been surveyed and summarized both at the higher level as well as at the low levels. In WSNs, the issue of having security and design of routing algorithms is very important to study the design properties like connectivity, node coverage and fault tolerance.

We have discussed different attacks that spoil the characteristics of that layer. We have also covered the countermeasures and potential solutions against those attacks, and mentioned some open research issues. Hopefully by reading the survey, the readers can have a better view of attacks and countermeasures in wireless sensor networks, and find their way to start secure designs for these networks.

### References


underwater sensor networks”, Proceedings of the Fourth
2002, pp. 54-62.
[5] Zaw Tun and Aung Htein Maw,(2008)," Worm hole
Attack Detection in Wireless Sensor networks”,
proceedings of world Academy of Science, Engineering
and Technology Volume 36, December 2008, ISSN
2070-3740.
[6] Khin Sandar Win, Department of Engineering Physics,
Mandalay Technological University, Pathein Gyi,
Mandalay,” Analysis of Detecting Wormhole Attack in
Wireless Networks”, World Academy of Science,
Engineering and Technology , 2008,pp.48-55
Wormhole Attacks, 14 Proceedings of the 11th Network
[8] W. Wang, B. Bhargava., Visualization of wormholes in
sensor networks, Proceedings of the 2004 ACM
Lightweight Countermeasure for the Wormhole attack in
multihop wireless network,” in International Conference
on Dependable Systems and Networks (DSN), 2005.
[10] D. Sheela, Nirmala, S. Sangita Nath and Dr. G
Mahadevan,” A Recent Technique to Detect Sink Hole
Attacks in WSN ”.
mobile agent routes for data fusion in distributed sensor
networks,” IEEE Transactions on Knowledge and Data
Networks, in: proc. Of SASN 2003. Fairfax, Virginia,
October 2003.
[14] Castro and Liskov, “Practical byzantine fault tolerance,”
in OSDI: Symposium on OperatingSystems Design and
Implementation. USENIX Association, Co-sponsored by
[15] A. Banerjea, "taxonomy of dispersity routing schemes
for fault tolerant real-time channels," in Proceedings of
detection in wireless ad hoc networks,"Department of
Computer Science, Rice University, Tech. Rep. TR01-
384, June 2002.
International Workshop on Peer-to-Peer Systems (IPTPS
’02).
sensor networks: Attacks and countermeasures”,
Elsevier's Ad Hoc Network Journal, Special Issue on