Taxonomy on Security Attacks on Self Configurable Networks

Noor Mohd, Singh Annapurna and H.S. Bhadauria

Govind Ballabh Pant Engineering College, Pauri Garhwal, Uttarakhand, India

Abstract: Designing an intrusion detection system for a mobile wireless system is technically a difficult task. Due to more mobile computing devices are coming into existence, in variable size, capabilities, mode of interaction and so on. One day mobile devices and its applications are omnipresent in the world. Mobile devices are using wireless technologies like Bluetooth, Infrared, Wibree, Zigbee, 802.11, IrDA, WiMax (802.16), Wireless Sensor Network (802.15) or ultrasound. These devices are using different technologies but one thing is common to them is that they are cooperative in nature. And due to this nature and their sophisticated applications they are vulnerable to threats and attacks. In the recent years numerous new attacks are identified which are not present in the wired networks. And wired networks intrusion detection system is completely failed to fix. This paper discusses the security attacks and intrusion detection systems methodology for self configurable networks.

Key words: Wireless Networks · Mobile Adhoc Networks · Wireless Sensor Networks · Self configurable networks · Intrusion detection system · Security attacks

INTRODUCTION

Security challenges emerge due to the ad hoc and dynamic nature of mobile ad hoc networks (MANET), in which devices do not know each other a priori, but still need to develop spontaneous interactions between themselves.

Adhoc networks nodes are free to move arbitrarily with different speeds [1] thus, the network topology may change randomly and at unpredictable times. Some or all of the nodes in an ad hoc network may rely on batteries or other exhaustible means for their energy [2, 3]. For these nodes, the most important system design optimization criteria may be energy conservation. Wireless links continue to have significantly lower capacity than infrastructured networks. In addition, the realized throughput of wireless communications-after accounting for the effects of multiple access, fading, noise and interference conditions, etc., is often much less than a radio's maximum transmission rate.

There are many applications of MANETs. As a matter of fact, any day-to-day application such as electronic email and file transfer can be considered to be easily deployable within an ad hoc network environment. Web services are also possible in case any node in the network can serve as a gateway to the outside world [4]. In this discussion, we need not emphasize wide range of military applications possible with ad hoc networks. Not to mention, the technology was initially developed keeping in mind the military applications, such as battlefield in an unknown territory where an infrastructure network is almost impossible to establish or maintain. In such situations, the ad hoc networks having self-organizing capability can be effectively used where other technologies either fail or cannot be deployed effectively.

The advances on miniaturization techniques and wireless communications have made possible the creation and subsequent development of the Wireless Sensor Networks (WSN) paradigm [5-7]. The main purpose of WSN is to serve as an interface to the real world, providing physical information such as temperature, light, radiation, etc. to a computer system [8-11]. The major difference between this type of networks and wired networks is their decentralized and specialized nature. In WSN, all its members collaborate towards the common

Corresponding Author: Noor Mohd, Govind Ballabh Pant Engineering College, Pauri Garhwal, Uttarakhand, India.
goal of obtaining or deducing certain physical information from their environment. Moreover, WSN is capable of self-organization, thus it can be deployed in a certain context without requiring the existence of a supporting infrastructure.

The functionality and behaviour of WSN are also different from another wireless network paradigm, Mobile Ad Hoc Network (MANET). First, all devices in WSN are totally autonomous, not controlled by human users. Also, those devices are much more constrained in terms of battery life and processing power, so it can only offer a simple and predefined set of tasks, whereas a MANET node is usually a PDA-like device with much more functionality and resources. In addition, the density of WSN is usually higher than in MANET.

The infrastructure of WSN can be divided into two parts, the data acquisition network and the data dissemination network [12-14]. The data acquisition network contains the sensor network "per se": sensor nodes and base stations. Sensor nodes are a collection of small devices with the task of measuring the physical data of its surroundings and base stations are powerful devices in charge of collecting data from the nodes and forwarding control information from the users [15-17]. On the other hand, the data dissemination network is a combination of wired and wireless networks that provides an interface of the data acquisition network to any user.

In addition to those traditional security issues, we observe that many general-purpose sensor network techniques (particularly the early research) assumed that all nodes are cooperative and trustworthy. This is not the case for most, or much of, real-world wireless sensor networking applications, which require a certain amount of trust in the application in order to maintain proper network functionality [18, 19].

In addition, there are many attacks designed to exploit the unreliable communication channels and unattended operation of wireless sensor networks. Furthermore, due to the inherent unattended feature of wireless sensor networks, we argue that physical attacks to sensors play an important role in the operation of wireless sensor networks [20].

The security of a network system can be provided with the help of intrusion prevention system and intrusion detection system [21-24]. Both techniques need to complement each other to provide a highly secure environment [25]. They play different roles in different states of the network. Security mechanism (X.800) is provided by intrusion prevention system and more useful in preventing outside attacks. When a node of a system is compromised, the attacker owns all its cryptographic information, so encryption and authentication cannot defend against a trusted but malicious user. Therefore, the role of intrusion detection is more important. And this is not an intelligent idea to load heavy applications on the tiny mobile devices for security. Proactive applications are consuming batteries on continuous basis but reactive security systems like intrusion detection system is a good solution for these kind of mobile systems, where cooperation is the primary goal.

Most of today’s wired IDSs, which rely on real-time traffic parse, filter, format and analysis, usually monitor the traffic at switches, routers and gateways. The lack of such traffic monitoring points makes traditional wired IDSs inadequate for infrastructure less wireless network platforms. There are also some characteristics of an infrastructure less wireless network such as dynamic topology, mobile/semi-mobile and immobile nodes, disconnected operations, problem of localization which seldom exist in the wired network.

**Attack Model**: Two kinds of threat models are discussed in infrastructure less wireless networks, one attack model is internal threat from trusted sources and external threat models from outside the network by unauthorized nodes. External threats are very easy to be detected. Internal attacks are posed by the internal trusted node which is compromised by the attacker. And it is very difficult to distinguish between a regular or malicious communication. In this section we will discuss the generalized attack models whether it is internal or external threat on the basis of layered architecture for communication.

**Attack Models in the MAC Layer**: The attacks on the MAC layer are also known as an unfair use of a transmission channel. For the wireless networks it is purely based on the fair share of radio waves. But an intruder or malicious node can prevent other nodes in the network from getting transparent share of the channel. This activity can be considered as a denial of service (DoS) attack against the neighbors which are participating in a fair competition for allocation of transmission channels in a contention based network. Since the competing neighbors are deprived of their fair share of the transmission channel. Possible methods for unfair use of the transmission channel are as follows:
Ignoring the MAC Protocol: Protocols like 802.11, uses request for transmission (RTS) and clear for transmission (CTS) mechanism to notify the neighbors that how long the transmission channel will be reserved by the node for successful transmission [26]. The availability of these protocols avoided the problem of collision [27]. But a misbehaving node can violate these protocols. Hence the competing neighbors are unable to get a fair share of channels [28]. This imposes a long delay at the output queues of the nodes and finally packets are timed out and get removed.

Jamming the Transmission Channel with Garbage: Garbage can consist of packets of unknown formats, violating the proper sequence of a transaction (e.g. sending a data packet without exchanging RTS and CTS) or simply random bits used as static noise by misbehaving nodes [29-31]. Garbage data may result in too many collisions and may consume a significant part of the available Channel capacity.

Malicious Flooding: Deliver unusually large amount of data or control packets to whole network or some targeted nodes [32-35]. We can distinguish two kinds of flooding attack. First one is the route request (RREQ) flooding attack. It ignores the network limitations for sending RREQ messages and sends a large number of RREQ packets with a maximum time to live (TTL) value addressing nodes that do not exist in the network.

The second is called data flooding attack. In this malicious node first sets up paths to all nodes in the network and then sends large volumes of useless data packets to all nodes along these paths, depleting in this way the available network bandwidth. Both attacks consume the available network resources and disallowing other nodes to communicate correctly.

Network Partition: A connected network is partitioned into sub networks where nodes in different sub networks cannot communicate even though a route between them actually does exist [36, 37].

Sleep Derivation: A node is forced to exhaust its battery power. It can be achieved by Denial of Service attack. Even it is not denial of service but sending the targeted node unnecessary request to process.

On-Off Attack: A malicious node may alternatively behave well and badly to stay undetected while disrupting services [38, 39]. Some time it acts as malicious and some time it acts as trusted node. So fooling the Intrusion detection system if present any in the network.

Attack Models in the Network Layer: The security threat on the network layer is called as anomaly in packet forwarding. Packet forwarding includes the data packets and control packets as well. This section is not considering the circuit switching based network because the research is based on wireless communication. This layer is the sophisticated and soft target of the attackers for both attack models internal and external threat. An anomaly in packet forwarding for different wireless networks takes the different forms. Some attacks are specific to the specific architecture and most of them are generalized for all heterogeneous wireless environments.

Blackhole Attack/Sinkhole Attack: In blackhole attack alias sinkhole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept [40-42]. In this way attacker node will always have the availability in replying to the route request and thus attract the whole traffic on the network and intercept the data packet and further it may retain it or drop it.

Wormhole Attack: A tunnel is created between two nodes that can be utilized to secretly transmit packets. Wormhole [45-48] is a term adopted to describe an attack against the routing protocol in which two cooperating malicious nodes create a tunnel between two points of the network. The attack is possible even if none hosts were compromised and even attacked network introduced a strong authentication and encryption algorithms. This is the most difficult attack to trace it and counter it.

Byzantine Attack: This attack is derived from Two Armies problem of Byzantine valley. Twoarmies, each led by ageneral, are preparing to attack a fortified city. The armies are encamped near the city, each on its own hill. A valley separates the two hills and the only way for the two generals to communicate is by sending messengers through the valley. Unfortunately, the valley is occupied by the city's defenders and there's a chance that any given messenger sent through the valley will be captured (this scenario assumes that while the two generals have agreed that they will attack, they haven't agreed upon a time for attack before taking up their positions on their respective hills).
The two generals must have their armies attack the city at the same time in order to succeed. They must thus communicate with each other to decide on a time to attack and to agree to attack at that time and each general must know that the other general knows that they have agreed to the attack plan. Because acknowledgement of message can be lost as easily as the original message, a potentially infinite series of messages are required to come to consensus.

In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets [49-51] which results in disruption or degradation of the routing services. It is hard to detect byzantine failures. The network would seem to be operating normally in the viewpoint of the nodes, though it may actually be showing Byzantine behavior.

**The Sybil Attack:** In this attack, a single node i.e. a malicious node will appear to be a set of nodes and will send incorrect information to a node in the network [42-44]. The incorrect information can be a variety of things, including the position of the nodes, signal strengths, making up nodes that do not exist.

**Denial of Service Attack:** A node is prevented from receiving and sending data packets to its destinations. Attacker sends the unnecessary data packets to targeted node to void its main services.

In this type of attack, an attacker attempts to prevent legitimate and authorized users from the services offered by the network. A denial of service (DoS) attack can be carried out in many ways. The classic way is to flood packets to any centralized resource present in the network so that the resource is no longer available to nodes in the network, as a result of which the network no longer operating in the manner it was designed to operate [53]. This may lead to a failure in the delivery of guaranteed services to the end users. Due to the unique characteristics of ad hoc wireless networks, there exist many more ways to launch a DoS attack in such a network, which would not be possible in wired networks. DoS attacks can be launched against any layer in the network protocol stack [54]. On the physical and MAC layers, an adversary could employ jamming signals which disrupt the on-going transmissions on the wireless channel [55]. On the network layer, an adversary could take part in the routing process and exploit the routing protocol to disrupt the normal functioning of the network.

For example, an adversary node could participate in a session but simply drop a certain number of packets, which may lead to degradation in the QoS being offered by the network. On the higher layers, an adversary could bring down critical services such as the key management service.

**Rushing Attack:** This kind of attack is applied on reactive routing protocols. In this an attacker that can forward ROUTE REQUESTs more quickly than legitimate nodes can do so, can increase the probability that routes that include the attacker will be discovered rather than other valid routes [56, 57]. This is called as rushing to find out route in order to incorporate attack on the targeted node.

**Packet Drop:** Packet drop is most common attack [58-60]. It is done not only individually but with the help of all kind of attacks including blackhole, denial of service and Sybil attack.

**Delay in Packet Transmissions:** An attacker is doing unnecessary delay for transferring the packets to the destination to disrupt the Quality of Service [47].

**Fabricated Route Messages:** Route messages with malicious contents are injected into the network [43]. Due to the cooperative nature of self configurable networks, this kind of attack is most dangerous and malicious contents are spreading throughout the networks via the trusted node and will destroy the complete network.

**False Source Route:** An incorrect route is advertised on the network, setting the route length to be the shortest, regardless where the destination is [61]. And vice a versa can also be applicable to forcefully adopt more vulnerable route.

**Cache Poisonings:** Information stored in routing tables is modified, deleted or injected with false information [62]. Spreading this information and misguiding the whole network.

**Selfishness:** A node is not serving as a relay node to other nodes[63]. It may be saving its battery for particular process to disrupt or probe the network.
**Attack Models in the Transport Layer:** The transport layer has very specific protocols including TCP, UDP and real time streaming protocols like SCTP and RSVP. But infrastructures less wireless networks are not designed to handle the real time streaming. Instead they use the service of UDP and TCP for data transfer. Though TCP has been extensively used for the wired network but is being used for mobile Adhoc network in the transport layer [64]. As there is no complementary protocol available for providing the connection oriented services in the infrastructure less wireless network. Though there is some principle difference in TCP for wired network and TCP for wireless network but basic functionality is same.

**Session Hijacking:** Session hijacking is a critical error and gives an opportunity to the malicious node to behave as a legitimate system. All the communications are authenticated only at the beginning of session setup. The attacker may take the advantage of this and commit session hijacking attack. At first, he or she spoofs the IP address of target machine and determines the correct sequence number. After that he performs a DoS attack on the victim. As a result, the target system becomes unavailable for some time. The attacker now continues the session with the other system as a legitimate system.

**Attacks using the TCP Segment Header**

**Denial of Service Attack:** There are various types of DoS attacks are possible. But for this chapter we consider the case of the TCP / IP header only.

**Guest/Remote to Local (R2L) Login Attack** *(Unauthorized Access from a Remote System):* An attacker, who does not have rights of authentication on a targeted node, gains local access to extract files from the system, or modifies data in transit to the system.

**Probing: Surveillance and Other Probing**

**Ping Sweep/ IP Sweep:** Ping (beacon signal) sweep is a technique used to identify which range of IP addresses map to live node. In this ICMP ECHO request are sent to multiple hosts. If a given address node is live, it will reply with an ICMP ECHO. A ping command is often used to verify that a network device/node is functioning or not.

**Port Sweep:** Port sweep is a method to probe a server or host for open ports and not the working ports to launch the zombie attack.

**SYN Scan:** SYN scan is another form of TCP scanning. The port scanner software generates raw IP packets and then monitors the responses from the targeted node. This scan type is called as "half-open handshaking". Exactly, as it never opens a full TCP connection. The port scanner software generates a SYN packet. If the targeted node port is open, it will reply with a SYN-ACK packet. The scanner node will reply with a RST packet and thus closing the connection before handshaking completed.

**SYN Scan with FIN:** SYN scans are not surreptitious enough; firewalls are present in general (for the wired network). Scanning and blocking packets in the form of SYN packets are possible by the firewall. Then FIN bit ON packets are able to pass through firewalls without any modification. Closed ports from the targeted node will reply to a FIN packet with an appropriate RST packet, whereas open targeted ports will ignore the packets.

**Attacks Using UDP Header**

**UDP Flood Attack:** UDP is a connectionless protocol and it does not require any connection setup procedure to transfer data [65]. A UDP Flood Attack is possible when an attacker sends a UDP packet to a random port on the victim system. When the victim system receives a UDP packet, it will determine what application is waiting on the destination port. When it realizes that there is no application that is waiting on the port, it will generate an ICMP packet of destination unreachable to the forged source address. If enough UDP packets are delivered to ports on the victim, the system will go down.

**Attack Models in the Application Service Layer:**
The application layer is more vulnerable compared with other layers. Application layer holds the attraction of the attacker because all needed information is present in this layer. This layer holds the user data and supports many protocols such as HTTP, SMTP, TELNET and FTP. But for Adhoc network environment. Application protocol may be differing according to the nature of the node. So this layer in Adhoc network is called as MANET traffic generation layer and in wireless Sensor network it is called as service layer. There are various forms of attacks are available for this layer but the most common attack types are discussed below.

**Masquerading:** A bogus registration is an active attack in which an attacker does a registration with a bogus care-of-address by masquerading itself as someone else [66]. By advertising fraudulent beacons, an attacker might
Table 1: Attack models on different layers

<table>
<thead>
<tr>
<th>Layer Attack</th>
<th>Attack Models on Application Layer</th>
<th>Attack Based on TCP segment Header</th>
<th>Session Hijacking, Denial of Service Attack, Probing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Masquerading, Repudiation, Data Corruption/Modification</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Layer Attack</th>
<th>Attack Models on Transport Layer</th>
<th>Attacks Based on UDP Header</th>
<th>Flood Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Black hole attack/Sinkhole attack, Wormhole attack, Byzantine attack, The Sybil attack, Denial of Service Attack, Rushing Attack, Packet Drop, Delay in Packet Transmissions, Fabricated route Network messages, False Source Route, Cache Poisonings, Selfishness</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Layer Attack</th>
<th>Attack Models on MAC layer Attacks</th>
<th>Ignoring the MAC protocol, Jamming the transmission channel with garbage, Malicious flooding, Network Partition, Sleep Derivation, On-Off Attack</th>
</tr>
</thead>
</table>

be able to attract a MN (mobile node) to register with the attacker as if MN has reached HA (home agent) or FA (foreign agent). Now, the attacker can capture sensitive personal or network data for the purpose of accessing network and may disrupt the proper functioning of network. It is difficult for an attacker to implement such type of attack because the attacker must have detailed information about the agent.

**Repudiation:** In simple terms, repudiation refers to the denial or attempted denial by a node involved in a communication of having participated in all or part of the communication [67]. Example of repudiation attack is a commercial system in which a selfish person could deny conducting an operation on a credit card purchase or deny any on-line transaction Non-repudiation is one of the important requirements for a security protocol in any communication network.

**Data Corruption/Modification:** It includes all kind of active attacks including data corruption and modification in original message [68].

**CONCLUSION**

In this paper we discussed the possible attack models in each layer for self configurable networks. Self configurable networks include mobile Adhoc networks, Wireless Sensor networks and Mesh networks. These self configurable networks are much popular among the researchers due their wide application in human life including monitoring, habitat monitoring, weather forecasting, earth quake forecasting and future possible ecommerce applications. These networks are cooperative networks so they can be deceived by the intruders. So, discussion of possible attacks leads the direction of security and safety of these networks.

**REFERENCES**


