IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

Vulnerabilities in Wireless Sensor Networks: Attacks and Countermeasures

Prajna SP[1], Pranav Kalidas[2], Pratheeka Karkera[3], Pratheeksha Rao[4], Reena Lobo[5]
Student, Department of Computer Science and Engineering[1,2,3,4]
Assistant Professor, Department of Computer Science of Engineering[5]
Alva's Institute of Engineering and Technology, Mijar, Mangalore, Karnataka, India

Abstract: *In wireless sensor networks, we look at routing security. There have been numerous sensor network routing protocols proposed, but none of them have been developed with security in mind. We propose security goals for sensor network routing, show how ad-hoc and peer-to-peer network attacks can be adapted into powerful sensor network attacks, introduce two new types of sensor network attacks—sinkholes and HELLO floods—and assess the security of all major sensor network routing protocols. We detail all of them as targets for debilitating attacks and offer countermeasures and design considerations. This is the first study of secure routing in sensor networks of its kind.*

Keywords: Wireless Sensor Networks

I. INTRODUCTION

Our research focuses on wireless sensor network routing security. Current approaches for sensor network routing protocols optimise for the nodes' restricted capabilities and the application-specific nature of the networks, but they ignore security. Despite the fact that these protocols were not created with security in mind, we believe it is vital to examine their security aspects. When the defence faces unsecured wireless communication, restricted node capabilities, and probable insider threats, and the adversaries may attack the network with powerful laptops that have high energy and long-range communication, developing a safe routing protocol is difficult.

In-network aggregation is one characteristic of sensor networks that challenges the design of a safe routing system. A secure routing system is often only necessary in more traditional networks to ensure message availability. An end-to-end security system such as SSH or SSL handles message integrity, authenticity, and confidentiality at a higher layer [1]. In more traditional networks, end-to-end security is achievable since intermediary routers are not required or desired to have access to message content.

Although link layer security methods can help mitigate some of the ensuing vulnerabilities, they are insufficient: our routing protocols will now be expected to do much more, and they must be built with this in mind.

II. NEED FOR SECURITY

Sensor networks and wireless mobile ad hoc networks (MANETs) have numerous uses in the military, homeland security, and other fields. Many sensor networks provide mission-critical functions. For such networks deployed in hostile situations, security is crucial, and security concerns continue to be a major roadblock to wider adoption of these wireless networks. MANET security challenges are more difficult to address than those faced by standard wired computer networks and the Internet. Due to the resource constraints of sensor nodes, providing security in sensor networks is considerably more difficult than in MANETs. Most sensor networks continually monitor their surroundings, and information other than the data being watched is frequently straightforward to discern. People's privacy is frequently violated as a result of such unwanted information leaks.[2]

III. SENSOR NETWORKS VS. AD-HOC WIRELESS NETWORKS

Ad-hoc wireless networks and wireless sensor networks have a lot in common. Multihop networking is the major communication mechanism in both, however there are numerous significant differences between the two. Sensor networks feature a more specific communication pattern than ad-hoc networks, which normally permit routing between any two nodes.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

The majority of sensor network traffic falls into one of three categories:

1. Many-to-one: A base station or aggregation point in the network receives sensor readings from several sensor nodes.
2. One-to-many: A single node (usually a base station) sends a query or control information to numerous sensor nodes in a multicast or flood fashion.
3. Local communication: Neighbouring nodes communicate with one another by sending localised messages.

A node can broadcast messages to all nearby nodes or send unicast messages to a single neighbour. Ad-hoc network nodes unit usually thought to possess restricted resources, however device nodes, as we have AN inclination to saw in Section two, unit even lots of affected. restricted energy is that the foremost pressing resource restriction of all. several device networks unit meant to be left unattended for extended periods of a while once preparation, creating battery recharge or replacement powerful or impractical. device network nodes oftentimes have trust connections that are not gift in many forms of networks three A node among typical radio vary is mentioned as a neighbour. [3]

Environmental events are often witnessed by neighbouring nodes in sensor networks. When each node responds by sending a packet to the base station, energy and bandwidth are lost. Sensor networks require in-network processing, aggregation, and duplicate removal to prune these redundant messages and save traffic and energy. This frequently needs node-to-node trust connections that are not normally expected in ad-hoc networks.

IV. Attacks on Sensor Network Routing

Because many sensor network routing protocols are fairly basic, they are sometimes vulnerable to attacks from the literature on ad-hoc network routing. The majority of sensor network Neighbouring layer attacks fall into one of the following categories:

- Spoofed, altered, or replayed routing information selective forwarding,
- Sinkhole attacks,
- Sybil attacks,
- Wormholes,
- Hello flood attacks,
- Acknowledgement spoofing.

4.1 Spoofed, Altered, or Replayed Routing Information

Targeting the routing information transferred between nodes is the most direct attack against a routing protocol. Adversaries may be able to construct routing loops, attract or repel network traffic, prolong or shorten source paths, generate false error messages, partition the network, raise end-to-end latency, and so on by faking, modifying, or replaying routing information.

4.2 Sinkhole Assaults

Sinkhole attacks prohibit the base station from receiving complete and accurate sensing data, posing a significant danger to higher-layer applications. Given the susceptibility of wireless connectivity, the fact that sensors are frequently deployed in open places, and the low processing and battery power of the sensors, it is especially serious for wireless sensor networks. Although certain secure or geographic-based routing systems are resistant to sinkhole attacks in some circumstances, others are not.

4.3. Sybil Attacks

Because of the broadcast nature of the wireless medium and the lack of central authority, wireless ad hoc networks are vulnerable to Sybil attacks. In a Sybil assault, an opponent falsely claims to have many fictitious identities known as Sybil nodes. This attack has the potential to disrupt data aggregation, voting-based procedures, fair resource allocation methods, misbehaviour detection, and routing algorithms in these networks. In this study, we give an overview of the most promising strategies for defending the three types of ad hoc networks against the Sybil attack, namely Mobile Ad hoc Networks, Wireless Sensor Networks, and Wireless Mesh Networks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

4.4. Wormholes

An attacker records a packet, or specific bits from a packet, at one point in the network, tunnels the data to another point in the network, and repeats the packet there. (In Section 2, we go through the wormhole assault in further depth.) In wireless networks, the wormhole attack can pose a severe danger, notably to various ad hoc network routing methods and location-based wireless security solutions. The wormhole puts the attacker in a powerful position, allowing them to further leverage any of the techniques listed above, such as gaining unauthorised access, disrupting routing, or launching a denial-of-service attack (DoS) [5]. We describe the overall mechanism of packet leashes for detecting wormhole assaults, as well as two other forms of leashes: geographic and temporal leashes. Finally, we devise TIK, a time-saving authentication system for use with temporal leashes.

4.5. HELLO Flood Attacks

The hello flood attack is a network layer assault in which an adversary who is not a legal node in the network floods hello requests to any genuine node using high transmission power, compromising the security of WSNs. The majority of current solutions for this type of attack are cryptographic, and therefore have a high processing complexity. As a result, they're not as good in terms of memory and battery life. In this paper, a strategy for detecting and preventing hello flood attacks based on the signal intensity of received Hello messages is proposed.

Based on the signal intensity of Hello messages provided by nodes, they were categorised as friend or stranger. Stranger nodes are further validated by sending a simple test packet; if the test packet reply arrives within a present time, it is considered valid; otherwise, it is considered malicious [6]. In ns-2, the technique is implemented by altering the AODV routing protocol. The algorithm's performance has been evaluated in a variety of network settings. In comparison to AODV with hello flood attack, simulation results demonstrate that the new algorithm performs better in terms of number of packet delivery ratio.

4.6 Acknowledgment Spoofing

Several sensor network routing algorithms rely on link layer acknowledgements, either implicitly or explicitly. An adversary can spoof link layer acknowledgments for "overheard" packets addressed to surrounding nodes due to the inherent broadcast medium. Convincing the sender that a weak link is strong or that a dead or disabled node is alive is one of the objectives. A routing protocol, for example, may use connection reliability to determine the next hop in a path. A sneaky technique of controlling such a scheme is to artificially reinforce a weak or dead link. Because packets delivered across weak or dead links are lost, an adversary might use acknowledgement spoofing to launch a selective forwarding attack by persuading the target node to send packets over those links. [7]

V. COUNTERMEASURES

Simple link layer encryption and authentication using a globally shared key can prevent the bulk of external attacks on sensor network routing technologies. Because nodes are unwilling to accept even a single attacker identity, the Sybil attack is no longer relevant. Because the adversary is barred from entering the topology, the majority of selective forwarding and sinkhole attacks are impossible. Authentication of link layer acknowledgements is now possible.

Wormhole attacks and HELLO flood assaults are two major types of attacks that aren't protected by link layer encryption and authentication methods. Although an adversary is prevented from joining the network, nothing prevents her from using a wormhole to tunnel packets sent by legitimate nodes in one part of the network to legitimate nodes in another part of the network in order to fool them into believing they are neighbours, or from a9mplifying an overheard broadcast packet with enough power to be received by every node in the network.

These techniques are demonstrated in the assaults against TinyOS beaconing detailed in Section 7.1, and link layer security features are powerless to stop them. If a wormhole is constructed, encryption may make some selective forwarding attacks against packets traversing the wormhole more difficult, but it can't stop "black hole" selective forwarding. In the event of insider attacks or compromised nodes, link layer security techniques using a globally shared key are absolutely worthless. Insiders can spoof or insert phoney routing information, create sinkholes, selectively route packets, use the Sybil attack, and broadcast HELLO floods to assault the network. To provide reasonable security against wormholes and insider attacks, more advanced defence techniques are required. In the next sections, we will focus on countermeasures to these attacks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

VI. Other Security Concerns

Security-energy assessment, data assurance, survivability, Trust, end-to-end security, Security and Privacy Support for data centric sensor networks (DCS), and node compromise distribution are some of the other security concerns [9]. Due to the unique characteristics of sensor networks, such as battery limitations, high failure probability nodes, easily compromised nodes, unreliable transmission media, and so on, it's critical to investigate these areas. There have only been a few ways available up to now, and further research is needed in these areas.

VII. Conclusion

Secure routing is critical for the acceptability and deployment of sensor networks in many applications; however, we've shown that the routing protocols currently proposed for these networks are insecure. Designing a sensor network routing protocol that meets our stated security criteria is left as an open problem. Although link layer encryption and authentication techniques may provide a decent initial line of defence against outsiders of the mote class, cryptography alone is insufficient. Because of the possibility of laptop-class attackers and insiders, as well as the limited applicability of end-to-end security methods, careful protocol design is also required.

References

[1]. Brad Karp and H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," in Proc. of the 6th ACM MobiCom, Aug 2000, pp. 243-254

[2]. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," in Proc. of the 1st IEEE Workshop on Sensor Network Protocols and Applications, May 2003, pp.1-15.

[3]. M. Ilyas and I. Magoub., Compact Wireless and Wired Sensing System, CRC Press, 2005

[4]. G. Acs and L. Buttyabv., "A Taxonomy of Routing Protocols for Wireless Sensor Networks," BUTE Telecommunication Department, Vol. LXII, pp 32-40, Jan 2007

[5]. D.B. Johnson, D.A. Maltz, Dynamic source routing in ad hoc wireless networks, in: T. Imielinski, H.F. Korth (Eds.), Mobile Computing, vol. 353, Kluwer Academic Publishers, Boston, 1996

[6]. Hongfa Wang, "A Robust Mechanism for Wireless Sensor Network Security", 4th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM '08), PP 1 –4, Oct 2008.

[7]. A. Karnik, K. Passerini ,"Wireless network security - A discussion from a business perspective", IEEE Wireless Telecommunications Symposium, pp:261 – 267, 2005.

[8]. Kerlof,C. and Wagner,D.," Secure routing in wireless sensor networks: Attacks and counter measures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Netwok Applications and Protocols , September 2003,pp.293-315

[9]. Zaw Tun and Aung Htein Maw,(2008),"Wormhole Attack Detection in Wireless Sensor networks", Proceedings of World Academy of Science ,Engineering and Technology,Volume 36,December 2008,ISSN 2070-3740.