Sensor in Wireless Networks-Threats & Security

Rahul Pareek, Deeksha Choudhary, Seema Nebhwani

Abstract— **The security of computer networks plays a strategic role in modern computer systems especially when we talk about Wireless Networking. We consider routing security in wireless networks. Many network routing protocols have been proposed, but none of them have been designed with security as a goal. We propose security goals for routing in sensor networks, show how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce two classes of novel attacks against sensor networks —sinkholes and HELLO floods, and analyze the security of all the major sensor network routing protocols. We describe crippling attacks against all of them and suggest countermeasures and design considerations.**

In order to enforce high protection levels against malicious attack, a number of software tools have been currently developed. Wireless sensor network has recently become a heated research topic due to its capability of detecting and preventing the attacks from malicious network users. A powerful sensor security for wireless network has been proposed in this paper.

.

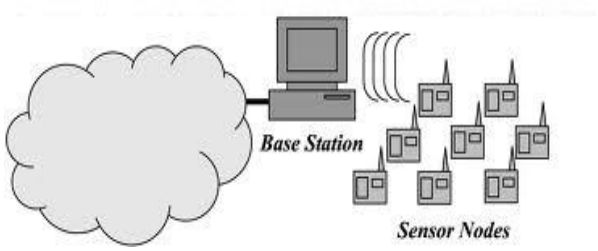
***Index Terms*—Sensor Networks, Sensor N/w Vs Ad-Hoc Network, Attacks in Senor N/w, Prevention.**

I. INTRODUCTION

Sensor Wireless Network Security:

Our focus is on routing security in wireless sensor networks. Current proposals for routing protocols in sensor networks optimize for the limited capabilities of the nodes and the application specific nature of the networks, but do not consider security. Although these protocols have not been designed with security as a goal, we feel it is important to analyze their security properties. When the defender has the liabilities of insecure wireless communication, limited node capabilities, and possible insider threats, and the adversaries can use powerful laptops with high energy and long range communication to attack the network, designing a secure routing protocol is non-trivial. Our assertion is that sensor network routing protocols must be designed with security in mind, and this is the only effective solution for secure routing in sensor networks. We make five main contributions. We propose threat models and security goals for secure routing in wireless sensor networks. We introduce two novel classes of previously undocumented attacks against sensor networks– sinkhole attacks and HELLO floods. We show, for the first time, how attacks against ad-hoc wireless networks and peer-to-peer networks. These attacks are relevant to some ad-hoc wireless networks as well be adapted into powerful attacks against sensor networks. We present the first detailed security analysis of all the Major routing protocols and energy conserving topology Maintenance algorithms for sensor networks.

We describe practical attacks against all of them that would defeat any reasonable security goals. We discuss countermeasures and design considerations for secure routing protocols in sensor networks.



Sensor Wireless Network

NECESSITY

Security incidents are rising at an alarming rate every year. As the complexity of the threats increases, so do the security measures required to protect networks. Data center operators, network administrators, and other data center professionals need to comprehend the basics of security in order to safely deploy and manage networks today.

OBJECTIVES

As time goes on, more and more new technology will be developed to further improve the efficiency of business and communications. At the same time, breakthroughs in Technology will provide even greater network security, Therefore, greater piece of mind to operate in cutting edge business environments. Provided that enterprises stay on top of this emerging technology, as well as the latest security threats and dangers, the benefits of networks will most certainly outweigh the risks.

II. SENSOR NETWORK

Sensor networks are the key to gathering the information needed by smart environments, whether in buildings, utilities, industrial, home, shipboard, transportation systems automation, or elsewhere. Recent terrorist and guerilla warfare countermeasures require distributed networks of sensors that can be deployed using, e.g. aircraft, and have self-organizing capabilities. In such applications, running wires or cabling is usually impractical. A sensor network is required that is fast and easy to install and maintain. Wireless sensor networks satisfy these requirements. Desirable functions for sensor nodes include: ease of installation, self-identification, self-diagnosis, reliability, time awareness for coordination with other nodes, some software functions and DSP, and standard control protocols and network interfaces

Manuscript received May 27, 2011.

Rahul Pareek, MCA, RTU/ Rajasthan College of Engineering for Women/ RCEW, Jaipur, India, 9460489537, (e-mail: dhruvpareek@gamil.com).

Deeksha Choudhary, MCA, RTU/ Rajasthan College of Engineering for Women / RCEW, Jaipur, India, 9460158595, (e-mail: deekshachoudhary23@yahoo.com).

Seema Nebhwani, MCA, RTU/ Rajasthan College of Engineering for Women /RCEW, Jaipur, India, 9887321975. (e-mail: seemanebhwani@yahoo.co.in).

SMART SENSOR: A smart sensor is a sensor that provides extra functions beyond those necessary for generating a correct representation of the sensed quantity. Included might be signal conditioning, signal processing, and decision-making/alarm functions. Objectives for smart sensors include moving the intelligence closer to the point of measurement; making it cost effective to integrate and maintain distributed sensor systems; creating a confluence of transducers, control, computation, and communications towards a common goal and seamlessly interfacing numerous sensors of different types.

VIRTUAL SENSOR: A virtual sensor is the physical sensor/transducer, plus the associated signal conditioning and digital signal processing (DSP) required obtaining reliable estimates of the required sensory information. The virtual sensor is a component of the smart sensor.

III. Sensor Networks vs AD-HOC Wireless Networks

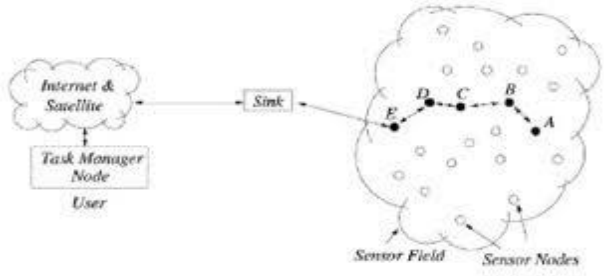
Wireless sensor networks share similarities with ad-hoc Wireless networks. The dominant communication method in both is multi-hop networking, but several important distinctions can be drawn between the two. Ad-hoc networks typically support routing between any pair of nodes whereas sensor networks have a more specialized communication pattern. Most traffic in sensor networks can be classified into one of three categories:

1) **Many-to-one**: Multiple sensor nodes send sensor readings to a base station or aggregation point in the network.

2) **One-to-many**: A single node (typically a base station) Multicasts or floods a query or control information to several sensor nodes.

3) **Local communication**: Neighboring nodes send localized messages to discover and coordinate with each other. A node may broadcast messages intended to be received by all neighboring nodes or unicast messages intended for a only single neighbor3.

Nodes in ad-hoc networks have generally been considered to have limited resources, sensor nodes are even more constrained. Nodes in sensor networks often exhibit trust relationships beyond those that are typically found in ad-hoc networks. Neighboring nodes in sensor networks often witness the same or correlated environmental events. If each node sends a packet to the base station in response, precious energy and bandwidth are wasted. To prune these redundant messages to reduce traffic and save energy, sensor networks require in-network processing, aggregation, and duplicate elimination. This often necessitates trust relationships between nodes that are not typically assumed in ad-hoc networks.



Ad-Hoc Network

IV. Problem Statement

Before diving into specific routing protocols, it helps to have a clear statement of the routing security problem. In the following sections we outline our assumptions about the underlying network, propose models for different classes of adversaries, and consider security goals in this setting.

A. **Network Assumptions**: Because sensor networks use wireless communications, we must assume that radio links are insecure. At the very least, attackers can eavesdrop on our radio transmissions, inject bits in the channel, and replay previously heard packets.

B. **Trust Requirements**: Since base stations interface a sensor network to the outside world, the compromise of a significant number of them can render the entire network useless. For this reason we assume that base stations are trustworthy, in the sense that they can be trusted if necessary and are assumed to behave correctly. Most, but not all routing protocols depend on nodes to trust messages from base stations. Aggregation points may be trusted components in certain protocols. Nodes may rely on routing information from aggregation points and trust that messages sent to aggregation points will be accurately combined with other messages and forwarded to a base station. Aggregation points are often regular sensor nodes.

C. **Threat Models**: An important distinction can be made between mote-class attackers and laptop-class attackers. In the former case, the attacker has access to a few sensor nodes with similar capabilities to our own, but not much more than this. In contrast, a laptop-class attacker may have access to more powerful devices, like laptops or their equivalent. Thus, in the latter case, malicious nodes have an advantage over legitimate nodes: they may have greater battery power, a more capable CPU, a high-power radio transmitter, or a sensitive antenna. An attacker with laptop-class devices can do more than an attacker with only ordinary sensor nodes. An ordinary sensor node might only be able to jam the radio link in its immediate vicinity, while a laptop-class attacker might be able to jam the entire sensor network using its stronger transmitter. A single laptop-class attacker might be able to eavesdrop on an entire network, while sensor nodes would ordinarily have a limited range. Also, laptop-class attackers might have a high bandwidth, low-latency communications channel not available to ordinary sensor nodes, allowing such attackers to coordinate their efforts.

*D. **Security Goals**: In the ideal world, a secure routing protocol should guarantee the integrity, authenticity, and availability of messages in the presence of adversaries of* arbitrary power. Every eligible receiver should receive all messages intended for it and be able to verify the integrity of every message as well as the identity of the sender. In our view, protection against eavesdropping is not an explicit security goal of a secure routing algorithm. Secrecy is usually most relevant to application data, and it is arguably not the responsibility of a routing protocol to provide it. However, we do consider it the responsibility of a routing protocol to prevent eavesdropping caused by misuse or abuse of the protocol itself. Eavesdropping achieved by the cloning or rerouting of a data flow should be prevented, for example.

V Attacks on Sensor Network Routing

Many sensor network routing protocols are quite simple, and for this reason are sometimes even more susceptible to attacks against general ad-hoc routing protocols. Most network layer attacks against sensor networks fall into one of the following categories:

A. **Spoofed, altered, or replayed routing information**: The most direct attack against a routing protocol is to target the routing information exchanged between nodes. By spoofing, altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc.

B. **Selective forwarding**: Multi-hop networks are often based on the assumption that participating nodes will faithfully forward receive messages. In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. A

simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet she sees. However, such an attacker runs the risk that neighboring nodes will conclude that she has failed and decides to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. An adversary interested in suppressing or modifying packets originating from a select few nodes can reliably forward the remaining traffic and limit suspicion of her wrongdoing.

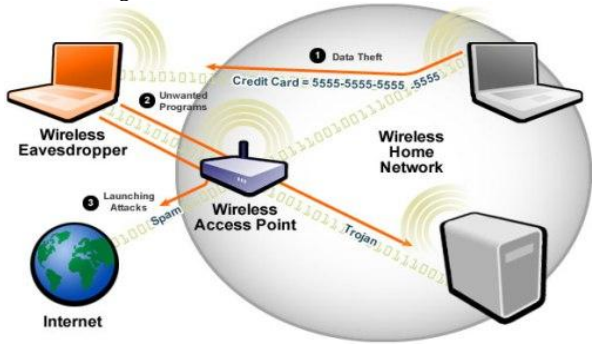
C. **Sinkhole attacks**: In a sinkhole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Because nodes on, or near, the path that packets follow have many opportunities to tamper with application data, sinkhole attacks can enable many other attacks. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm.

D. **Sybil attack***:* In a Sybil attack, a single node presents multiple Identities to other nodes in the network. The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes such as distributed storage, disparity and multipath routing, and topology maintenance. Replicas, storage partitions, or routes believed to be using disjoint nodes could in actuality be using a single adversary presenting multiple identities. Sybil attacks also pose a significant threat to geographic routing protocols. Location aware routing often requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets. It is only reasonable to expect a node to accept but a single set of coordinates from each of its neighbors, but by using the Sybil attack an adversary can "be in more than one place at once".

E. **Wormholes**: In the wormhole attack, an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part5. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them. However, wormhole attacks more commonly involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker.

F. **HELLO flood attack**: We introduce a novel attack against sensor networks the HELLO flood. Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false: a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor.

G. **Acknowledgement spoofing**: Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgements. Due to the inherent broadcast medium, an adversary can spoof link layer acknowledgments for "overheard" packets addressed to neighboring nodes. Goals include convincing the sender that a weak link is strong or that a dead or disabled node is alive.



Attack on Sensor Network

VI. Prevention

A. **Outsider attacks and link layer security**: The majority of outsider attacks against sensor network routing protocols can be prevented by simple link layer encryption and authentication using a globally shared key. The Sybil attack is no longer relevant because nodes are unwilling to accept even a single identity of the adversary. The majority of selective forwarding and sinkhole attacks are not possible because the adversary is prevented from joining the topology. Link layer acknowledgements can now be authenticated. Major classes of attacks not countered by link layer encryption and authentication mechanisms are wormhole attacks and HELLO flood attacks. 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 to convince them they are neighbors or by amplifying an overheard broadcast packet with sufficient power to be received by every node in the network.

B. **Sybil attack**: An insider cannot be prevented from participating in the network, but she should only be able to do so using the identities of the nodes she has compromised. Using a globally shared key allows an insider to masquerade as any node. Identities must be verified. In the traditional setting, this might be done using public key cryptography, but generating and verifying digital signatures is beyond the capabilities of sensor nodes.

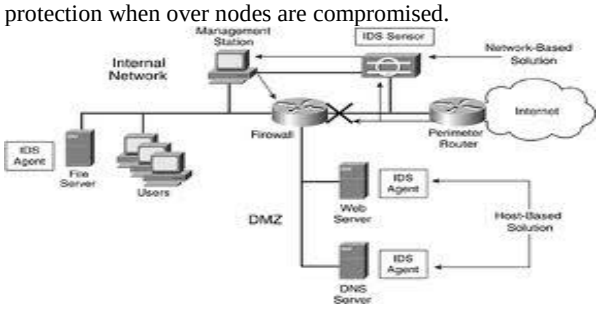
One solution is to have every node share a unique symmetric key with a trusted base station. Two nodes can then use a Needham-Schroeder like protocol to verify each other's identity and establish a shared key. A pair of neighboring nodes can use the resulting key to implement an authenticated, encrypted link between them. In order to prevent an insider from wandering around a stationary network and establishing shared keys with every node in the network, the base station can reasonably limit the number of neighbors a node is allowed to have and send an error message when a node exceeds it.

C. **HELLO flood attacks**: The simplest defense against HELLO flood attacks is to verify the bidirectional of a link before taking meaningful action based on a message received over that link. Not only does it verify the bidirectional of the link between two nodes, but even if a well-funded adversary had a highly sensitive receiver or had wormholes to a multiple locations in the network, a trusted base station that limits the number of verified neighbors for each node will still prevent HELLO flood attacks on large segments of the network when a small number of nodes have been compromised.

D. **Wormhole and sinkhole attacks**: Wormhole and sinkhole attacks are very difficult to defend against, especially when the two are used in combination. Wormholes are hard to detect because they use a private, out-of-band channel invisible to the underlying sensor network. Sinkholes are difficult to defend against in protocols that use advertised information such as remaining energy or an estimate of end-to-end reliability to construct a routing topology because this information is hard to verify. Routes that minimize the hop-count to a base station are easier to verify, however hop-count can be completely misrepresented through a wormhole in Tiny OS, sinkholes are easy to create because there is no information for a defender to verify.

E. **Leveraging global knowledge**: A significant challenge in securing large sensor networks is their inherent self-organizing, decentralized nature. When the network size is limited or the topology is well-structured or controlled, global knowledge can be leveraged in security mechanisms.

F. **Selective forwarding**: Even in protocols completely resistant to sinkholes, wormholes, and the Sybil attack, a compromised node has a significant probability of including itself on a data flow to launch a selective forwarding attack if it is strategically located near the source or a base station. Multipath routing can be used to counter these types of Selective forwarding attacks. Messages routed over paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most compromised nodes and still offer some probabilistic protection when over nodes are compromised.



Security in Sensor Network

VII. Conclusion

As time goes on, more and more new technology will be developed to further improve the efficiency of business and communications. At the same time, breakthroughs in technology will provide even greater network security, therefore, greater piece of mind to operate in cutting edge business environments. Provided that enterprises stay on top of this emerging technology, as well as the latest security threats and dangers, the benefits of networks will most certainly outweigh the risks. Secure routing is vital to the acceptance and use of sensor networks for many applications, but we have demonstrated that currently proposed routing protocols for these networks are insecure. We leave it as an open problem to design a sensor network routing protocol that satisfies our proposed security goals. Link layer encryption and authentication mechanisms may be a reasonable first approximation for defense against mote-class outsiders, but cryptography is not enough to defend against laptop-class adversaries and insiders: careful protocol design is needed as well.

References

1. http://en.wikipedia.org/wiki/wirelessNetwork_security
2. http://www.interhack.net/pubs/wirelessnetwork-security
3. http://e-articles.info/e/s/s/WirelessNetwork-security/
4. ijns.femto.com.tw/contents/ijns-v10-n1/ijns-v10-n1.html
5. pnbiit.com/download/JulSep09.pdf