WIRELESS SENSOR NETWORK SECURITY ANALYSIS

Hemanta Kumar Kalita[1] and Avijit Kar[2]

[1]Department of Computer Engineering, Jadavpur University, Kolkata, India
hemanta91@yahoo.co.in
[2]Department of Computer Engineering, Jadavpur University, Kolkata, India
avijit.kar@gmail.com

ABSTRACT

The emergence of sensor networks as one of the dominant technology trends in the coming decades has posed numerous unique challenges to researchers. These networks are likely to be composed of hundreds, and potentially thousands of tiny sensor nodes, functioning autonomously, and in many cases, without access to renewable energy resources. Cost constraints and the need for ubiquitous, invisible deployments will result in small sized, resource-constrained sensor nodes. While the set of challenges in sensor networks are diverse, we focus on security of Wireless Sensor Network in this paper. We propose some of the security goal for Wireless Sensor Network. Further, security being vital to the acceptance and use of sensor networks for many applications; we have made an in depth threat analysis of Wireless Sensor Network. We also propose some countermeasures against these threats in Wireless Sensor Network.

KEYWORDS

Wireless Sensor Network (WSN), Security

1. INTRODUCTION

We use the term sensor network to refer to a heterogeneous system combining tiny sensors and actuators with general purpose computing elements. The Application domains of Wireless Sensor Network are diverse due to the availability of micro-sensors and low-power wireless communications. Unlike the traditional sensors, in the remote sensor network, a vast numbers of sensors are densely deployed. These sensor nodes will perform significant signal processing, computation, and network self-configuration to achieve scalable, robust and long-lived networks[5]. More specifically, sensor nodes will do local processing to reduce communications, and consequently, energy costs. We believe that most efficient and adaptive routing model for WSN is cluster based hierarchical model. For a cluster based sensor network, the cluster formation plays a key factor to the cost reduction, where cost refers to the expense of setup and maintenance of the sensor networks.

In this paper, we will take a more in-depth look at security in WSN and discuss counter measures.

2. WSN ARCHITECTURE

In a typical WSN we see following network components –

- Sensor motes (Field devices) – Field devices are mounted in the process and must be capable of routing packets on behalf of other devices. In most cases they characterize or control the process or process equipment. A router is a special type of field device that does not have process sensor or control equipment and as such does not interface with the process itself.

- Gateway or Access points – A Gateway enables communication between Host application and field devices.
- Network manager – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.
- Security manager – The Security Manager is responsible for the generation, storage, and management of keys.

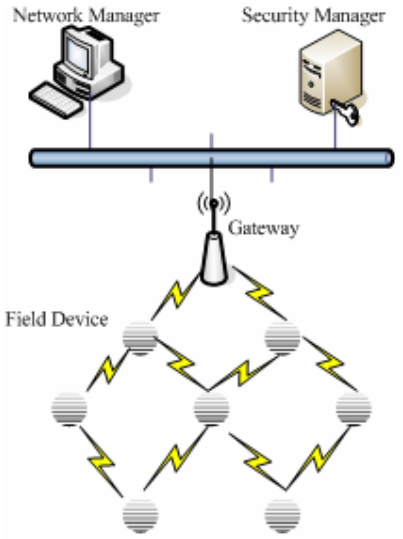

Figure 1 WSN Architecture

3. WSN SECURITY ANALYSIS

Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. Attackers can eavesdrop on our radio transmissions, inject bits in the channel, replay previously heard packets and many more. Securing the Wireless Sensor Network needs to make the network support all security properties: confidentiality, integrity, authenticity and availability. Attackers may deploy a few malicious nodes with similar hardware capabilities as the legitimate nodes that might collude to attack the system cooperatively. The attacker may come upon these malicious nodes by purchasing them separately, or by "turning" a few legitimate nodes by capturing them and physically overwriting their memory. Also, in some cases colluding nodes might have high-quality communications links available for coordinating their attack. Sensor nodes may not be tamper resistant and if an adversary compromises a node, she can extract all key material, data, and code stored on that node. While tamper resistance might be a viable defense for physical node compromise for some networks, we do not see it as a general purpose solution. Extremely effective tamper resistance tends to add significant per-unit cost, and sensor nodes are intended to be very inexpensive [1] [2] [3] [4].

We identify and categorize attacks in Wireless Sensor Network as follows:

3.1. Denial of Service

Denial of Service (DoS) is any event that diminishes or eliminates a network's capacity to perform its expected function [16].

Attack 3.1 DoS/Physical Layer/Jamming. Jamming. To jam a node or set of nodes, in this case, this is simply the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network. Jamming the channel with an interrupting signal.

Attack 3.2 DoS/Physical Layer/Tampering. Physical Tampering. Nodes are vulnerable to physical harm, or tampering (i.e. reverse engineering).

Attack 3.3 DoS/Data Link Layer/Collision.

Attack 3.4 DoS/Data Link Layer/Exhaustion.

Attack 3.5 DoS/Data Link Layer/Unfairness.

Attack 3.6 DoS/Network Layer/Neglect and Greed.

Attack 3.7 DoS/Network Layer/Homing.

Attack 3.8 DoS/Network Layer/Spoofing. Misdirection. In this type of attack 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.

Attack 3.9 DoS/Network Layer/Black Holes.

Attack 3.10 DoS/Network Layer/Flooding.

Attack 3.11 DoS/Transport Layer/Flooding.

Attack 3.12 DoS/Transport Layer/De-synchronization.

3.2. Interrogation

Attack 3.13 Interrogation/Data Link Layer.

3.3. Sybil

Sybil attack is defined as a "malicious device illegitimately taking on multiple identities". Using the Sybil attack [7], an adversary can "be in more than one place at once" as a single node presents multiple identities to other nodes in the network which can significantly reduce the effectiveness of fault tolerant schemes such as distributed storage [8], dispersity [9] and multipath. It may be extremely difficult for an adversary to launch such an attack in a network where every pair of neighboring nodes uses a unique key to initialize frequency hopping or spread spectrum communication. Sybil attacks also pose a significant threat to geographic routing protocols.

Attack 3.14 Sybil/Physical Layer.

Attack 3.15 Sybil/Data Link Layer/Data Aggregation.

Attack 3.16 Sybil/Data Link Layer/Voting. Stuffing the ballot box of a voting scheme, for example.

Attack 3.17 Sybil/Network Layer.

3.4. Wormhole

In the wormhole attack [10], an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An adversary could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can create a sinkhole: since the adversary on the other side of the wormhole can artificially provide a high-quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive.

Attack 3.18 Wormhole/Network Layer. A routing attack where an adversary convinces a network node of a shorter, or zero, path to the base station, for example, and can disrupt the network in this manner.

3.5. Sinkhole (Black hole)

Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm and 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 (selective forwarding, for example).

Attack 3.19 Sinkhole/Network Layer.

3.6. Manipulating Routing Information

Attack 3.20 Manipulating Routing Information/Network Layer.

3.7. Selective Forwarding

In a selective forwarding attack, malicious nodes behaves like black hole and may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. However, such an attacker runs the risks that neighboring nodes will conclude that she has failed and decide 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.

Attack 3.21 Selective Forwarding/Network Layer.

3.8. 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 and begin exchanging information with the nodes.

Attack 3.22 Hello Flood/Network Layer.

3.9. 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 3.23 Acknowledgement spoofing.

3.10. Cloning

Attack 3.24 Cloning/Application Layer.

3.11. Impersonation

Attack 3.25 Node Replication. Also called Multiple Identity, Impersonation. An attacker seeks to add a node to an existing sensor network by copying (replicating) the node ID of an existing sensor node. Node replication attacks can occur if an adversary can copy the node identification of a network node. In this manner packets could be corrupted, misrouted or deleted, and if this adversary could perform this replication it is possible that cryptographic keys could be disclosed.

3.12. Eavesdropping

Attack 3.26 Monitor and eavesdropping. Also called confidentiality. By listening to the data, the adversary could easily discover the communication contents. Network traffic is also susceptible to monitoring and eavesdropping. This should be no cause for concern given a robust security protocol, but monitoring could lead to attacks similar to those previously described. It could also lead to wormhole or black hole attacks.

3.13. Traffic Analysis

Attack 3.27 Traffic Analyses. Traffic analysis attacks are forged where the base station is determinable by observation that the majority of packets are being routed to one particular node. If an adversary can compromise the base station then it can render the network useless.

3.14. Mote Class

Also called Insider Attacks. The attackers have an authorized participant in the sensor network. Insider attacks may be mounted from either compromised sensor nodes running malicious code or adversaries who have stolen the key material, code, and data from legitimate nodes, and who then use one or more laptop-class devices to attack the network. Mote-class attacker [6] has access to a few sensor nodes with similar capabilities to our own, but not much more than this. Using ordinary sensors attacker might only be able to jam the radio link in its immediate vicinity.

Attack 3.28 Mote-class/Control of Sensor Node. Malicious programs, access cryptographic keys.

3.15. Invasive

Attack 3.29 Invasive. Reverse engineering, probing. Extract keys, new code, software vulnerabilities.

3.16. Non-Invasive

Attack 3.30 Non-Invasive. Mote not physically tampered. Side-channel attacks – Differential power analysis.

3.17. Laptop Class

Also called Outsider Attacks. The attacker has no special access to the sensor network. Laptop class attacker may have access to more powerful devices, like laptops or their equivalent which supersede the legitimate nodes when deployed for action: they may have greater battery power, a more capable CPU, a high-power radio transmitter, or a sensitive antenna. 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. 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.

Attack 3.31 Laptop-class/Passive Eavesdropping.

Attack 3.32 Laptop-class/Traffic Injection.

3.18. Attack on Protocols

Attack 3.33 Key Management.

Attack 3.34 Reputation Assignment Scheme.

Attack 3.35 Data Aggregation.

Attack 3.36 Time Synchronization.

Attack 3.37 Intrusion Detection Systems.

4. COUNTER MEASURES

In this section, we discuss some of the counter measures.

4.1. 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. Major classes of attacks not countered by link layer encryption and authentication mechanisms are wormhole attacks and HELLO flood attacks because, 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.

Link layer security mechanisms using a globally shared key are completely ineffective in presence of insider attacks or compromised nodes. Insiders can attack the network by spoofing or injecting bogus routing information, creating sinkholes, selectively forwarding packets, using the Sybil attack, and broadcasting HELLO floods. More sophisticated defense mechanisms are needed to provide reasonable protection against wormholes and insider attacks. We focus on countermeasures against these attacks in the remaining sections.

4.2. The Sybil attacks

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 (possibly even nonexistent) 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. Thus, when a node is compromised, it is restricted to (meaningfully) communicating only with its verified neighbors. This is not to say that nodes are forbidden from sending messages to base stations or aggregation points multiple hops away, but they are restricted from using any node except their verified neighbors to do so. In addition, an adversary can still use a wormhole to create an artificial link between two nodes to convince them they are neighbors, but the adversary will not be able to eavesdrop on or modify any future communications between them.

4.3. HELLO flood attacks

The simplest defense against HELLO flood attacks is to verify the bi directionality of a link before taking meaningful action based on a message received over that link. The identity verification protocol is sufficient to prevent HELLO flood attacks. Not only does it verify the bidirectional 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.

4.4. 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. When routes are established simply based on the reception of a packet as in TinyOS beaconing or directed diffusion, sinkholes are easy to create because there is no information for a defender to verify. A technique for detecting wormhole attacks is presented in [10], but it requires extremely tight time synchronization and is thus infeasible for most sensor networks. Because it is extremely difficult to retrofit existing protocols with defenses against these attacks, the best solution is to carefully design routing protocols in which wormholes and sinkholes are meaningless.

4.5. 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. Consider a relatively small network of around 100 nodes or less. If it can be assumed that no nodes are compromised during deployment, then after the initial topology is formed, each node could send information such as neighboring nodes and its geographic location (if known) back to a base station. Using this information, the base station(s) can map the topology of the entire network. To account for topology changes due to radio interference or node failure, nodes would periodically update a base station with the appropriate information. Drastic or suspicious changes to the topology might indicate a node compromise, and the appropriate action can be taken. We have discussed why geographic routing can be relatively secure against wormhole, sinkhole, and Sybil attacks, but the main remaining problem is that location information advertised from neighboring nodes must be trusted. A compromised node advertising its location on a line between the targeted

node and a base station will guarantee it is the destination for all forwarded packets from that node. Probabilistic selection of a next hop from several acceptable destinations or multipath routing to multiple base stations can help with this problem, but it is not perfect. When a node must route around a "hole", an adversary can "help" by appearing to be the only reasonable node to forward packets to. Sufficiently restricting the structure of the topology can eliminate the requirement for nodes to advertise their locations if all nodes' locations are well known.

4.6. 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 whenever nodes are compromised. However, completely disjoint paths may be difficult to create. Braided paths [11] may have nodes in common, but have no links in common (i.e., no two consecutive nodes in common). The use of multiple braided paths may provide probabilistic protection against selective forwarding and use only localized information. Allowing nodes to dynamically choose a packet's next hop probabilistically from a set of possible candidates can further reduce the chances of an adversary gaining complete control of a data flow.

4.7. Authenticated broadcast and flooding

If we have base stations trustworthy, adversaries must not be able to spoof broadcast or flooded messages from any base station. This requires some level of asymmetry: since every node in the network can potentially be compromised, no node should be able to spoof messages from a base station, yet every node should be able to verify them. Authenticated broadcast is also useful for localized node interactions. Many protocols require nodes to broadcast HELLO messages to their neighbors. These messages should be authenticated and impossible to spoof. Proposals for authenticated broadcast intended for use in a more conventional setting either use digital signatures and/or have packet overhead that well exceed the length of typical sensor network packet. TESLA [12] is a protocol for efficient, authenticated broadcast and flooding that uses only symmetric key cryptography and requires minimal packet overhead. SPIN [13] and gossiping algorithms [14], [15] are techniques to reduce the messaging costs and collisions which still achieve robust probabilistic dissemination of messages to every node in the network.

4.8. OSI Layer wise threats and countermeasures

In this section, we discuss some of the known threats and countermeasures classifying in different OSI layers.

Physical Layer: In Table 1, we describe Physical Layer Threats & Countermeasures in case of Wireless Sensor Network.

Table 1 Physical Layer Threats and Countermeasures

Threat	Countermeasure
Interference	Channel hopping and Blacklisting
Jamming	Channel hopping and Blacklisting
Sybil	Physical Protection of devices
Tampering	Protection and Changing of key

Data-link Layer: In Table 2, we describe Data-Link Layer Threats & Countermeasures in case of Wireless Sensor Network.

Table 2 Data-link Layer Threats and Countermeasures

Threat	Countermeasure
Collision	CRC and Time diversity
Exhaustion	Protection of Network ID and other information that is required to joining device
Spoofing	Use different path for re-sending the message
Sybil	Regularly changing of key
De-synchronization	Using different neighbors for time synchronization
Traffic analysis	Sending of dummy packet in quite hours; and regular monitoring WSN network
Eavesdropping	Key protects DLPDU from Eavesdropper

Network Layer: In Table 3, we describe Network Layer Threats & Countermeasures in case of Wireless Sensor Network.

Table 3 Network Layer Threats and Countermeasures

Threat	Countermeasure
Wormhole	Physical monitoring of Field devices and regular monitoring of network using Source Routing. Monitoring system may use Packet Leach techniques.
Selective forwarding	Regular network monitoring using Source Routing
DoS	Protection of network specific data like Network ID etc. Physical protection and inspection of network.
Sybil	Resetting of devices and changing of session keys.
Traffic Analysis	Sending of dummy packet in quite hours; and regular monitoring WSN network.
Eavesdropping	Session keys protect NPDU from Eavesdroppers.

5. CONCLUSION

Security in Wireless Sensor Network is vital to the acceptance and use of sensor networks. In particular, Wireless Sensor Network product in industry will not get acceptance unless there is a fool proof security to the network. In this paper, we have made a threat analysis to the Wireless Sensor Network and suggested some counter measures. 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] S. Sharma, "Energy-efficient Secure Routing in Wireless Sensor Networks", Dept of Computer Science and Engineering, National Institute of Technology Rourkela, Rourkela, Orissa, 769 008, India, 2009.

[2] D. Boyle, T. Newe,"Securing Wireless Sensor Networks: Security Architectures", Journal of Networks, 2008, 3 (1).

[3] X. Du, H. Chen, "Security in Wireless Sensor Networks", IEEE Wireless Communications, 2008.

[4] J. Granjal, R. Silva, J. Silva, "Security in Wireless Sensor Networks", CISUC UC, 2008.

[5] Y. Zou, K. Chakrabarty, "Sensor deployment and target localization based on virtual forces", INFOCOM 2003. Twenty- Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, Volume: 2, Pages: 1293 - 1303, April 2003.

[6] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California at Berkeley.

[7] J. R. Douceur, "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), March 2002.

[8] Castro and Liskov, "Practical byzantine fault tolerance," in OSDI: Symposium on Operating Systems Design and Implementation. USENIX Association, Co-sponsored by IEEE TCOS and ACM SIGOPS, 1999.

[9] A. Banerjea, "A taxonomy of dispersity routing schemes for fault tolerant real-time channels," in Proceedings of ECMAST, vol. 26, May 1996, pp.129-148.

[10] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002.

[11] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," Mobile Computing and Communications Review, vol. 4, no. 5, October 2001.

[12] A. Perrig, R. Szewczyk, V.Wen, D. Culler, and J. Tygar, "SPINS: Security protocols for sensor networks," in Proceedings of Mobile Networking and Computing 2001, 2001.

[13] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," Wireless Networks, vol. 8, no. 2-3, pp. 169-185, 2002.

[14] M.-J. Lin, K. Marzullo, and S. Masini, "Gossip versus deterministic flooding: Low message overhead and high reliability for broadcasting on small networks, Tech. Rep. CS1999-0637, 18, 1999.

[15] L. Li, J. Halpern, and Z. Haas, "Gossip-based ad hoc routing," in IEEE Infocom 2002, 2002.

[16] Mona Sharifnejad, Mohsen Shari, Mansoureh Ghiasabadi and Sareh Beheshti, A Survey on Wireless Sensor Networks Security, SETIT 2007.