IJCSMS International Journal of Computer Science & Management Studies, Vol. 11, Issue 01, May 2011
ISSN (Online**): 2231 –5268**
www.ijcsms.com

Security Threats in Wireless Sensor Networks

Sushma[1], Deepak Nandal[2], Vikas Nandal[3]

[1]Asstt. Prof, HIT Asodha, (India)
sushma21dalal@gmail.com

[2]Student, P.D.M. Bahadurgarh, (India)
sinceredeepaknandal@yahoo.co.in

[3]Asstt. Prof, U.I.E.T. Rohtak, (India)
nandalvikas@gmail.com

Abstract

Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. Wireless sensor networks are characterized by severely constrained computational and energy resources, and an ad hoc operational environment. Wireless sensor networks (WSN) are currently receiving significant attention due to their unlimited potential. However, it is still very early in the lifetime of such systems and many research challenges exist. This paper studies the security aspects of these networks.

Keywords: *Data Authenticity, WSN, Attacks on sensor network, Spoofed.*

1. Introduction

Wireless Sensor Networks (WSN) are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed Algorithms, programming models, data management, security and social factors. Wireless sensor network applications include ocean and wildlife monitoring, manufacturing machinery performance monitoring, building safety and earthquake monitoring, and many military applications. An even wider spectrum of future applications is likely to follow, including the monitoring of highway traffic, pollution, wildfires, building security, water quality, and even people's heart rates. A major benefit of these systems is that they perform in-network processing to reduce large streams of raw data into useful aggregated information. Because sensor networks pose unique challenges, traditional security techniques used in traditional Networks cannot be applied directly. *First*, to make sensor networks economically viable, sensor devices are limited in their energy, computation, and communication capabilities. *Second*, unlike traditional networks, sensor nodes are often deployed in accessible areas, presenting the added risk of physical attack. And *third*, sensor networks interact closely with their physical environments and with people, posing new security problems. Consequently, existing security mechanisms are inadequate, and new ideas are needed.

2. Security Issues and Goals

2.1. Data Confidentiality

Confidentiality means keeping information secret from unauthorized parties. A sensor network should not leak sensor readings to neighboring networks. In many applications (e.g. key distribution) nodes communicate highly sensitive data. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality. Since public-key cryptography is too expensive to be used in the resource constrained sensor networks, most of the proposed protocols use symmetric key encryption methods. The creators of tiny Sec argue that cipher block chaining (CBC) is the most appropriate encryption scheme for sensor networks. They found RC5 and Skipjack to be most appropriate for software implementation on embedded microcontrollers. The default block cipher in tiny Sec is Skipjack. SPINS uses RC6 as its cipher.

2.2. Data Authenticity

IJCSMS International Journal of Computer Science & Management Studies, Vol. 11, Issue 01, May 2011
ISSN (Online**): 2231 –5268**
www.ijcsms.com

In a sensor network, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. Data authentication prevents unauthorized parties from participating in the network and legitimate nodes should be able to detect messages from unauthorized nodes and reject them. In the two-party communication case, data authentication can be achieved through a purely symmetric mechanism: The sender and the receiver share a secret key to compute a message authentication code (MAC) of all communicated data. When a message with a correct MAC arrives, the receiver knows that it must have been sent by the sender. However, authentication for broadcast messages requires stronger trust assumptions on the network nodes. The creators of SPINS contend that if one sender wants to send authentic data to mutually entrusted receivers, using a symmetric MAC is insecure since any one of the receivers know the MAC key, and hence could impersonate the sender and forge messages to other receivers. SPINS constructs authenticated broadcast from symmetric primitives, but introduces asymmetry with delayed key disclosure and one-way function key chains. LEAP uses a globally shared symmetric key for broadcast messages to the whole group. However, since the group key is shared among all the nodes in the network, an efficient reeking mechanism is defined for updating this key after a compromised node is revoked. This means that LEAP has also defined an efficient mechanism to verify whether a node has been compromised.

2.3. Data Integrity

Data integrity ensures the receiver that the received data is not altered in transit by an adversary. Note that Data Authentication can provide Data Integrity also.

2.4. Data Freshness

Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages. A common defense is to include a monotonically increasing counter with every message and reject messages with old counter values. With this policy, every recipient must maintain a table of the last value from every sender it receives. However, for RAM constrained sensor nodes, this defense becomes problematic for even modestly sized networks. Assuming nodes devote only a small fraction of their RAM for this neighbor table, an adversary replaying broadcast messages from many different senders can fill up the table. At this point, the recipient has one of two options: ignore any messages from senders not in its neighbor table, or purge entries from the table. Neither is acceptable; the first creates a DOS attack and the second permits replay attacks.

Some Researchers contend that protection against the replay of data packets should be provided at the application layer and not by a secure routing protocol as only the application can fully and accurately detect the replay of data packets (as opposed to retransmissions, for example). Whereas some authors reason that by using information about the network's topology and communication patterns, the application and routing layers can properly and efficiently manage a limited amount of memory devoted to replay detection.

Mostly Researchers have identified two types of freshness: weak freshness, which provides partial message ordering, but carries no delay information, and strong freshness, which provides a total order on a request-response pair, and allows for delay estimation. Weak freshness is required by sensor measurements, while strong freshness is useful foretime synchronization within the network.

2.5. Robustness and Survivability

The sensor network should be robust against various security attacks, and if an attack succeeds, its impact should be minimized. The compromise of a single node should not break the security of the entire network.

3. Attacks on sensor network routing

Many sensor network routing protocols are Quite simple, and for this reason are sometimes Susceptible to attacks from the literature on routing in ad-hoc networks. Most network layer attacks against sensor networks fall into one of the following categories:

1. Spoofed, altered, or replayed routing Information
2. Selective forwarding
3. Sinkhole attacks
4. Sybil attacks
5. Wormholes
6. HELLO flood attacks

3.1. Spoofed: altered, or replayed routing Information

IJCSMS International Journal of Computer Science & Management Studies, Vol. 11, Issue 01, May 2011
ISSN (Online**): 2231 –5268**
www.ijcsms.com

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.

3.2. 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. Selective forwarding attacks are typically most effective when the attacker is explicitly included on the path of a data flow. However, it is conceivable an adversary overhearing a flow passing through neighboring nodes might be able to emulate selective forwarding by jamming or causing a collision on each forwarded packet of interest.

3.3. Sinkhole attacks

In a sinkhole attack, the adversary 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 (selective forwarding, for example). Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. For instance; an adversary could spoof or replay an advertisement for an extremely high quality route to a base station. Some protocols might actually try to verify the quality of route with end-to-end acknowledgements containing reliability or latency information. In this case, a laptop-class adversary with a powerful transmitter can actually provide a high-quality route by transmitting with enough power to reach the base station in a single hop, or by using a wormhole attack discussed in Section 6.5. Due to either the real or imagined high-quality route through the compromised node, it is likely each neighboring node of the adversary will forward packets destined for a base station through the adversary, and also propagate the attractiveness of the route to its neighbors. Effectively, the adversary creates a large ‘‘sphere of influence’’, attracting all traffic destined for a base station from nodes several (or more) hops away from the compromised node.

3.4. The 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’’.

3.5. 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 part. 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.

3.6. HELLO flood attack

We introduce a novel attack against sensor networks: the HELLO flood. Many protocols

IJCSMS International Journal of Computer Science & Management Studies, Vol. 11, Issue 01, May 2011
ISSN (Online): 2231 –5268
www.ijcsms.com

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.

4. Countermeasures

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. 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. 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 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 (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.

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. However, this countermeasure is less effective when an adversary has a highly sensitive receiver as well as a powerful transmitter. Such an adversary can effectively create a wormhole to every node within range of its transmitter/receiver. Since the links between these nodes and the adversary are bidirectional, the above approach will unlikely being able to locally detect or prevent a HELLO flood? One possible solution to this problem is for every node to authenticate each of its neighbors with an identity verification protocol using a trusted base station. If the protocol sends messages in both directions over the link between the nodes, HELLO floods are prevented when the adversary only has a powerful transmitter because the protocol verifies the bi-directionality of the link. Although this does not prevent a compromised node with a sensitive receiver and a powerful transmitter from authenticating itself to a large number of nodes in the network, an observant base station may be able to detect a HELLO flood is imminent. Since such an adversary is required to authenticate itself to every victim before it can mount an attack, an adversary claiming to be a neighbor of an unusually large number of the nodes will raise an alarm.

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 hat 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 Tiny OS 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, 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 which avoid routing race conditions and make these attacks less meaningful. For example, one class of protocols resistant to these attacks is geographic routing protocols. Protocols that

IJCSMS International Journal of Computer Science & Management Studies, Vol. 11, Issue 01, May 2011
ISSN (Online**): 2231 –5268**
www.ijcsms.com

construct a topology initiated by a base station are most susceptible to wormhole and sinkhole attacks.

Geographic protocols construct a topology on demand using only localized interactions and information and without initiation from the base station. Because traffic is naturally routed onwards the physical location of a base station, it is difficult to attract it elsewhere to create a sinkhole. A wormhole is most effective when used to create sinkholes or artificial links that attract traffic. Artificial links are easily detected in geographic routing protocols because the ‘‘neighboring’’ nodes will notice the distance between them is well beyond normal radio range.

5. Ultimate limitations of secure multi hop routing

An ultimate limitation of building a multi hop routing topology around a fixed set of base stations is that those nodes within one or two hops of the base stations are particularly attractive for compromise. After a significant number of these nodes have been compromised, all is lost. This indicates that clustering protocols like LEACH where cluster-heads communicate directly with a base station may ultimately yield the most secure solutions against node compromise and insider attacks. Another option may be to have a randomly rotating set of ‘‘virtual’’ base stations to create an overlay network. After a set of virtual base stations have been selected, a multi hop topology is constructed using them. The virtual base stations then communicate directly with the real base stations. The set of virtual base stations should be changed frequently enough to make it difficult for adversaries to choose the ‘‘right’’ nodes to compromise.

6. Conclusion

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 alone is not enough. The possible presence of laptop-class adversaries and insiders and the limited applicability of end-to- end security mechanisms necessitate careful protocol design as well.

References:

[1] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar. SPINS: Security Protocols for Sensor Networks. *In The Seventh Annual International Conference on Mobile Computing and Networking (MobiCom 2001),2001*.

[2] Sasha Slijepcevic, Miodrag Potkonjak, Vlasios Tsiatsis, Scott Zimbeck, Mani B. Srivastava. On Communication Security in Wireless Ad-Hoc Sensor Networks. *In The Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), 2002*.

[3] 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*.

[4] Jeffery Undercoffer, Sasikanth Avancha, Anupam Joshi and John Pinkston. In Security for Sensor Networks.

[5] Chris Karlof David Wagner. In Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures.

[6] Wadaa, S. Olariu, L. Wilson, M. Eltoweissy, K. Jones. On Providing Anonymity in Wireless Sensor Networks. *In Proceedings of the Tenth International Conference on Parallel and Distributed Systems (ICPADS'04).*

[7] Chris Karlof, Naveen Sastry, David Wagner. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. *ACM SenSys 2004, November 3-5, 2004*.

[8] Sencun Zhu, Sanjeev Setia, Sushil Jajodia. LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. *In The Proceedings of the 10th ACM conference on Computer and communications security 2003*.

[9] Alan Mainwaring, Joseph Polastre, Robert Szewczyk, and David Culler. Wireless sensor networks for habitat monitoring. *In First ACM International Workshop on Wireless Sensor Networks and Applications, 2002*.

[10] K. Ishida, Y. Kakuda, T. Kikuno, A routing protocol for finding two node-disjoint paths in computer networks, in:International Conference on Network Protocols, 1992, pp.340–347.