International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Protocols Security for Wireless Sensor Networks

Parli B. Hari[1], Monika[2]

[1]Department of Computer Science, Indira Gandhi University, Rewari, Haryana

Abstract: ***As wireless sensor networks are growing fast so they need for effective security mechanisms as well. Sensor networks interact with sensitive data and operate in a hostile unattended environment, hence security concerns be addressed from the beginning of the network design. Due to resource and computing constraints, the biggest challenge in sensor network is to provide security in routing protocols. Many sensor network routing protocol have been proposed, but a very few have been designed with security as a goal. Asymmetric cryptographic algorithms are not suitable for sensor network providing security, as sensor nodes has limited computation, power and storage resources. On the other hand, it is not feasible to replace the batteries of thousands of sensor nodes, hence sensing, computing and communication protocols must be made as energy efficient as possible. There is currently enormous research potential in the field of wireless sensor network security. Thus, we need to be familiar with the current research in this field.***

Keywords: security, attacks, integrity, authentication, confidentiality

1. Introduction

The emerging field of wireless sensor networks combines sensing, computation, and communication into a single tiny device. The concept of wireless sensor networks is based on a simple equation:

Sensing + CPU + Radio = Thousands of potential applications

As soon as people understand the capabilities of a wireless sensor network, hundreds of applications spring to mind. It seems like a straightforward combination of modern technology. A vision is emerging of the convergence of wireless communications, embedded sensing and processing devices with distributed algorithms into the field of wireless sensor networks (WSNs). The proponents of this emerging technology envision a future in which environments from nature reserves to cities are instrumented with disposable computing nodes, each with an onboard radio transceiver, battery, environmental sensors and processing capabilities.

As shown in Figure 1, a WSN usually consists of hundreds or thousands of nodes scattered over a sensor field [1]. These nodes sometimes referred to as motes, collect their own sensed data and forward it in a multi-hop fashion to a sink, sometimes referred to as a base station or a gateway.

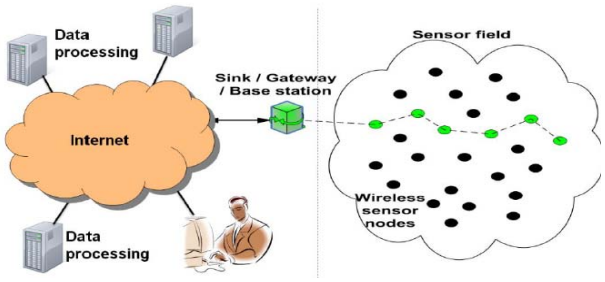

Figure 1.Wireless Sensor Network Architecture

Wireless sensor network research grew out of the distributed sensor networks project at the Defense Advanced Projects Research Agency (DARPA) [2], although the technology of the 1970s limited processing and communications and restricted the nodes to large form factors. With the exponential progress and cost reduction in microprocessing during the 1990s and 2000s, many new applications for WSN deployment emerged. The Amorphous Computing project [3] envisioned highly generic, cheap and indistinguishable miniature devices, operating by analogy to the individual cells of biological systems.

2. Attack in Different Application Domains

We consider in advance the intensions of potential attackers. WSN is liable to face attack in different patterns.

2.1 Military Networks

A military network is the key driver for WSN security, and much of the early research on sensor networks was funded by military agencies [6]. Military WSN Research is still ongoing via agencies such as the UK Ministry of Defence (MoD).

2.1.1 Logistics

WSN systems have been proposed for logistical tracking systems, both for delivery scheduling for customers and for business optimization. They can also be used to assure regulatory compliance; SecuriFood [7] uses embedded sensors to provide an audit trail ensuring frozen or chilled food has had a sufficient cold chain throughout transit to the final retailer.

2.1.2 Vehicular Networks

WSN concepts have been proposed for integration into cars and roadside systems, as part of Vehicular Ad-Hoc Networks (VANETs) [8]. Potential applications for VANETs include traffic behaviour monitoring, road and congestion charging, and vehicle tracking and recognition.

2.1.3 Environment Monitoring

Sensor networks have been proposed for a variety of environmental monitoring applications, for example soil quality analysis, or pollution monitoring within oceans, or to protect rare animals in desert terrain [9].

2.2 Nature of Wireless Sensor Networks Security

The broad goals of security engineering in the WSN, and indeed in any general communications system, typically involve the provision of a system with some combination of the following key properties [10]:

1) **Confidentiality:** The ability to keep the contents of a message secret and prevent its disclosure.
2) **Integrity:** Protecting a message from alteration in transit.
3) **Availability:** Ensuring communication services cannot be denied or suppressed by attackers.
4) **Authentication:** Ensuring that communications come from the entity that they claim and not a malicious imposter.

Roman [11] identifies intrinsic security of the nodes, protocols and the communication protocols of the sink as data acquisition security, as distinguished from data dissemination security, which is concerned with the security of the access network and physical terminals on which users access the output data.

2.2.1 Security Assumption

(i) Variation in capability

(ii) Fundamental Assumptions

(a) Lack of Channel Confidentiality
(b) Lack of Availability of Channel
(c) Lack of Integrity on Channel
(d) Trusted Base Station
(e) Possibility of Node Capture
(f) Compromise of Node Key Information

2.3 Threat and Common Attacks

The most insidious threats in a WSN are those which show an insight into the protocols comprising the active stack and operate upon its highest layers to put control undetected into the attacker's hands. Several attacks do not outwardly disrupt network functioning but make it possible for the attacker to gradually increase their level of control to enable a later attack. The seminal analysis of the WSN threat environment is Karlof and Wagner's paper [12], which provides an attack taxonomy concentrating on routing and network-layer attacks.

2.3.1 Selective Forwarding

In a selective forwarding attack, nodes fail to keep up their obligations to relay traffic for other nodes, and instead some traffic is silently discarded. Although this may appear on first consideration indistinguishable from node failure, a selective forwarding attack is more subtle in that a node participates in route formation as usual but fails to complete delivery when requested by other nodes.

2.3.2 Sinkhole

A sinkhole attack occurs when a node combines selective forwarding with route modification or fraudulent route formation; attempting to influence routing state held in other nodes so as to draw traffic into it. The sinkhole can be converted into a blackhole by dropping the inbound traffic that has been drawn to the node.

2.3.3 Sybil Attack

The Sybil attack [13] occurs when a single physical node impersonates additional identities (its sybil identities). For example, a malign node may forge randomly generated addresses in order to participate as multiple virtual nodes in routing or MAC protocols. It is a general problem in distributed systems, but especially severe in sensor networks since reliance on trusted parties to establish and vouch for identity is difficult due to the distance of nodes from a trusted authority such as the sink and the energy expense of dense party-to-party exchanges. The sybil attack allows compromise of multihop routing protocols.

2.3.4 Resource Consumption and Denial of Services

Resource consumption attacks are those which attempt to exhaust physical or virtual limited resources such as battery power or security descriptors. An example would be the conceptsleep deprivation attack [14] in which unintended media-access control interactions are used to exploit protocol rules to deplete batteries earlier than intended. A related attack is a denial-of-service (DOS) attack, which is an attack upon system availability.

2.4 Asymmetric Channel Attack

The HELLO flood attack [12] is a denial-of-service attack which can be mounted by an attacker with greater transmission range than network nodes. By using a powerful transceiver to globally broadcast a high-quality route advertisement proclaiming itself as a base station, recipients are tricked into sending packets to a neighbor which is unreachable, as the reverse channel is unavailable to the limited radio of a conventional mote.

2.5 Wormhole Attack

The wormhole attack occurs when the attacker exploits heterogeneity to attack the network. It occurs in a network in which the attacker deploys a pair of malicious devices with a private out-of-band, low-latency, point-to-point channel between them. These devices tunnel all traffic received at one endpoint to the other and rebroadcast it at the remote endpoint. The attack is highly insidious in that it allows the network to function undisturbed as long as the attacker wishes, albeit with a distorted topology which does not match the physical placement of nodes.

3. Protocols Security

3.1 Security Primitives and Resources

It is important to consider the security resources and primitives that are commonly deployed and available upon current and future WSN nodes. There is a heavy reliance upon cryptographic approaches, in order to protect the confidentiality and integrity of data messages transmitted [15]. However, it is important to remember that many attacks upon WSNs, particularly those that attempt to compromise availability, cannot be countered solely via cryptographic protection of the data packets.

3.2 Key Management

Although the security primitives can establish the security priorities of confidentiality, integrity and authenticity between the channel established between arbitrary node endpoints, they require the existence of appropriate cryptographic keys at the endpoints. It is worth considering that end-to-end encryption schemes in which intermediate nodes cannot access or modify the message preclude aggregation to suppress redundant messages and therefore impose a capacity and energy burden on the network. Therefore, nodes' having an individual key shared only with the base station on deployment is impractical for most situations, as it precludes the required interaction and collaboration.

3.3 LEAP (Localised Encryption and Authentication Protocol)

The Localised Encryption and Authentication Protocol (LEAP) [16] is a protocol which attempts to make key management more flexible, relating it to the requirements of a particular communications relationship. Since keys have fundamentally different requirements depending on their communications intent, number of involved parties, persistence of relationships, a multi-level keying scheme is required, tailored to each class of traffic. LEAP features four classes of keys; individual (shared only with the base station), group (network-wide key), cluster keys (for a node and all its reception peers) and pair wise (for one-to-one relations between node pairs).

3.4 SNEP (Secure Network Encryption Protocol)

SNEP (Secure Network Encryption Protocol) is a protocol which provides encryption, authentication, integrity, and guarantees of data freshness between a pair of communicating nodes that hold a shared symmetric key, while requiring only an 8 byte increase in packet header size. SNEP uses a symmetric master key to derive encryption key (kencr) and authentication key (kmac). A key establishment and distribution scheme must ensure that if is held privately between the communicating pairs and not disclosed or revealed to outsiders. Nodes also hold a frame counter for the unique interaction with the peer.

3.5 TINYSEC

Replacement for the unfinished SNEP, known as TinySec [4]. Inherently it provides similar services, including authentication, message integrity, confidentiality and replay protection. A major difference between TinySec and SNEP is that there are no counters used in TinySec. Generally, the security of CBC-MAC is directly related to the length of the MAC. TinySec specifies a MAC of 4 Bytes, much less than the conventional 8 or 16 Bytes of previous security protocols. In the context of sensor networks this is not detrimental [4]. TinySec, a lightweight, generic security package that developers can easily integrate into sensor network applications. TinySec will cover the basic security needs of all but the most security critical applications. In conventional networks, message authenticity, integrity, and confidentiality are usually achieved by an end-to-end security mechanism such as SSH , SSL [17], or IPSec [18] because the dominant traffic pattern is end-to-end communication; intermediate routers only need to view message headers and it is neither necessary nor desirable for them to have access to message bodies.

This is not the case in sensor networks. The dominant traffic pattern in sensor networks is many-to-one, with many sensor nodes communicating sensor readings or network events over a multihop topology to a central base station. However, neighbouring nodes in sensor networks often witness the same or correlated environmental events, and 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 use in-network processing such as aggregation and duplicate elimination [19, 20]. Since in-network processing requires intermediate nodes to access, modify, and suppress the contents of messages. End-to-end security mechanisms between each sensor node and the base station guarantee the authenticity, integrity, and confidentiality of these messages. End-to-End security mechanisms are also vulnerable to certain denial of service attacks. If message integrity is only checked at the final destination, the network may route packets injected by an adversary many hops before they are detected. This kind of attack will waste precious energy and bandwidth. Link-layer security architecture can detect unauthorized packets when they are first injected into the network. Link-layer security mechanisms have been proposed for wired networks to resist similar denial of service attacks [21].

3.6 ZigBee Security

The concept of a "Trust Center" is introduced in the specification. Generally the ZigBee coordinator performs this duty. This trust center allows other devices to join the network and also distributes the keys. There are three roles played: (i) Trust manager, whereby authentication of devices requesting to join the network is done
(ii) Network manager, maintaining and distributing network keys, and
(iii) Configuration manager, enabling end-to-end security between devices [22].

It operates in both Residential Mode and Commercial Mode. The Trust Center running residential Mode is used for low security residential applications. Commercial Mode is designed for high security commercial applications. In Residential Mode, the Trust Center will allow devices to join the network, but does not establish keys with the network devices. It therefore cannot periodically update keys and allows for the memory cost to be minimal, as it cannot scale with size of the network. In commercial mode, it establishes and maintains keys and freshness counters with every device in the network, allowing centralized control and update of keys. This results in a memory cost that could scale with the size of the network [22].

3.7 SM (Security Manager)

A new method of key agreement, whereby, when a new device joins network, the Security Manager (SM) gives static

domain parameters such as at the base station, the order of the curve and the elliptic curve coefficients [23]. After calculating a public key using the base point and a private key, the device sends a public key to the SM. Therefore the SM would have the public key list for all the devices in the network. They define two security levels (medium and high), based on the devices power and security policies. These two levels are defined by either normal or polynomial basis calculations. Elliptic Curve Cryptography (ECC) algorithms offer reasonable computational loads and smaller key lengths for equivalent security than other techniques. These smaller key lengths reduce the size of message buffers and reduce implementation cost of protocols. The EC-MQV (Menezes-Qu- Vanstone) scheme is more advanced than the Diffie-Hellman scheme, and the main idea is to prevent the man-in-the middle attack and perform authentication of key holders. Under this scheme, each side of the communication holds two keys. Devices in the network use initial trust parameters (pre-deployed recognition function) to establish the public key and ephemeral public key, which are in turn used for secure communication of the data payloads. The overhead here will depend on the number of bits chosen for the elliptic curve system. An elliptical curve algorithm provides the same security for 160 bit key lengths as a symmetric algorithm can for 128 Byte lengths [23].

4. Conclusion

SPINS is one of the secure and efficient sensor network protocol. LEAP is a protocol that survives in the face of security attacks and that the effects of any attacks may be minimized. TINYSEC is a stronger and energy efficient protocol. In ZIGBEE protocol, concept of a “trust center” is introduced. SM uses the EC-MQV scheme for key establishment, that is more advanced and main idea is to prevent the man-in-middle attack.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," in *IEEE Communications Magazine*, 2002, pp. 102-114.
[2] R. Lacoss, Strawman Design of a DSN (Distributed Sensors Networks) to Detect and Track Low Flying Aircraft in *Proceedings of the Distributed Sensor Nets Workshop*, pp. 41-52, Dec. 1978.
[3] H. Abelson, D. Allen, D. Coore, C. Hanson, G. Homsy, J. Thomas F. Knight, R. Nagpal, E. Rauch, G. J. Sussman, and R. Weiss, *Amorphous computing Communications of The ACM*, vol. 43, pp. 74-82, May 2000.
[4] C.Karlof, N.Sastry, D.Wagner, “TinySec: A link layer security architecture for wireless sensor networks”, In Proceedings of the 2nd International conference on embedded networked sensor systems, pp.162–175, Baltimore, MD, USA, November 2004.
[5] I-H. Huang, W. J. Tzeng, S.-W. Wang, C.-Z. Yang,“Design and implementation of a mobile SSH protocol”, pp. 1-4, TENCON, Nov. 2006.
[6] R. Lacoss, Strawman *Design of a DSN (Distributed Sensors Networks) to Detect and Track Low Flying Aircraft in Proceedings of the Distributed Sensor Nets Workshop*, pp. 41-52, Dec. 1978.
[7] R. Riem-Vis, Cold *Chain Management using an Ultra Low Power Wireless Sensor Network WAMES: Workshop on Applications of Mobile Embedded Systems*, 2004.
[8] M. Nekovee, *Sensor networks on the road: the promises and challenges of vehicular ad hoc networks and grids in Workshop on Ubiquitous Computing and e-Research*, 2005.
[9] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. S. Peh, and D. Rubenstein, *Energy-efficient computing for wildlife tracking: design tradeoffs and early 216 experiences with ZebraNet ACM SIGPLAN Notices*, vol. 37, pp. 96-107, Oct. 2002.
[10] R. Anderson, *Security engineering. Wiley New York*, 2001.
[11] R. Roman, J. Zhou, and J. Lopez, *On the security of wireless sensor networks Proc. Int. Conference on Computational Science and its Applications (ICCSA 2005)*, LNCS, vol. 3482, pp. 681-690, 2005.
[12] C. Karlof and D. Wagner, *Secure routing in wireless sensor networks: attacks and countermeasures Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293-315, 2003.
[13] J. Douceur, *The Sybil Attack in Peer-to-Peer Systems* (P. Druschel, F. Kaashoek, and A. Rowstron, eds.), vol. 2429 of Lecture Notes in Computer Science, pp. 251-260, Springer Berlin, 2002.
[14] F. Stajano and R. Anderson, *The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks IEEE Computer*, vol. 35, no. 4, pp. 22-26, 2002.
[15] C. Karlof, N. Sastry, and D.Wagner, TinySec: *a link layer security architecture for wireless sensor networks in SenSys 2004*: *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, (New York, NY,USA), pp. 162-175, ACM, Nov. 2004.
[16] S. Zhu, S. Setia, and S. Jajodia, LEAP: *efficient security mechanisms for largescale distributed sensor networks in CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, (New York, NY, USA), pp. 62-72, ACM, 2003.
[17] OpenSSL. http://www.openssl.org.
[18] *Security architecture for the Internet Protocol*, RFC 2401, November 1998.
[19] Samuel Madden, Michael J. Franklin, Joseph M.Hellerstein, and Wei Hong, “TAG: A tiny aggregation service for ad-hoc sensor networks”, *In Proceedings of the 5th symposium on operating system design and implementation (OSDI)*, pp. 131-146, December 9-11,2002.
[20] Samuel R. Madden, Robert Szewczyk, Michael J. Franklin, and David Culler, “*Supporting aggregate queries over ad-hoc wireless sensor networks”, 4th IEEE Workshop on mobile computing and systems applications*, pp. 49, 2002.
[21] Lyes Khelladi, Yacine Challal, Abdelmadjid Bouabdallah, Nadjib Badache, *“On security issues and challenges in embedded systems: challenges and solutions”, International journal of information and computer security* 2, vol. 2, pp. 140-174, 2008.
[22] ZigBee Alliance ZigBee *Security Specification Overview [online*
resentations/zigbee_security_layer_technical_overview.pdf
[23] Heo, J., Hong, “Efficient and authenticated key agreement mechanism in low-rate WPAN environment”, International Symposium on wireless pervasive computing, pp. 1-5, Phuket, Thailand 16 – 18 January 2006, IEEE 2006