Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 7, July 2013, pg.55 – 58

SURVEY ARTICLE

A Survey on Security Issues in Wireless Sensor Network

H.N. Pratihari
Department of Electronics & Communication Engineering
Centurion University of Technology & Management, Parlakhemundi- 761211
hnpratihari@rediffmail.com

Abstract— Sensor networks are key network to the creation of smart spaces, which embed information technology in everyday home and work environments. The miniature wireless sensor nodes, or motes, developed from low-cost off- the-shelf components at University of California, Berkeley, as part of its smart dust projects, establish a self- organizing sensor network when dispersed into an environment. The privacy and security issues posed by sensor networks represent a rich field of research problems. We consider routing security in wireless sensor networks. Many sensor 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 analyse the security of all the major sensor network routing protocols. Improving network hardware and software may address many of the issues, but others will require new supporting technologies.

Key Terms: - WSN, Security; Network; Routing; Privacy

I. INTRODUCTION

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 analyse 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.

One aspect of sensor networks that complicates the design of a secure routing protocol is in-network aggregation. In more conventional networks, a secure routing protocol is typically only required to guarantee message availability. Message integrity, authenticity, and confidentiality are handled at a higher layer by an end-to-end security mechanism such as SSH or SSL. End-to-end security is possible in more conventional networks because it is neither necessary nor desirable for intermediate routers to have access to the content of messages. However, in sensor networks, in-network processing makes end-to-end security mechanisms harder to deploy because intermediate nodes need direct access to the content of the messages [1]. The rapid progress of wireless communication and embedded micro-sensing MEMS technologies has made wireless sensor networks possible. Such environments may have many inexpensive wireless nodes, each capable of collecting, storing, and processing environmental information and communicating with neighbour nodes. In the past, sensors are connected by wire lines. Today, this environment is combined with the novel ad hoc networking technology to facilitate inter-sensor communication [3]. The flexibility of installing and configuring a sensor network is thus

greatly improved. Recently, a lot of research activities have been dedicated to sensor networks, including design issues related to the physical and media access layers [5] and routing and transport protocols [3]. Localization and positioning applications of wireless sensor networks are discussed in [2, 4].

II. PRIVACY OF SENSED DATA

Sensor networks are tools for collecting information, and an adversary can gain access to sensitive information either by accessing stored sensor data or by querying or eavesdropping on the network. Adversaries can use even seemingly innocuous data to derive sensitive information if they know how to correlate multiple sensor inputs. For example, an adversary that gains access to both the indoor and outdoor sensors of a home may be able to isolate internal noise from external noise and thus extract details about the inhabitants' private activities.

III. MALICIOUS USE OF COMMODITY NETWORKS

The proliferation of sensor networks will inevitably extend to criminals who can use them for illegal purposes. For example, thieves can spread sensors on the grounds of a private home to detect the inhabitants' presence. If the sensors are small enough, they can also plan them on computers and cell phones to extract private information and passwords. With widespread use, the cost and availability barriers that discourage such attacks will drop [6].

IV. ADAPTIVE LOCAL ROUTING

Adaptive Local Routing for cooperative signal processing we assume that an application level algorithm or outside agent will determine what cooperative function is needed and trigger the network formation process. In the following section, the term ``network`` refers specifically to a connected set of sensors that detected a common target. Before describing the network formation algorithm, a few remarks on the basic categories of environmental stimuli and cooperative functions are warranted.

In general, environmental stimuli can be separated into two major categories:

I. Near-field (NF)
II. Far-field (FF).

Near-field stimuli have short range relative to the baseline width of sensor groups within detectable distance. Signal propagation is dominated by the line-of-sight component; therefore SNR of sensor data can be modeled in the form: k d-r, where d is the distance between the sensor and the signal source and k and r are constant determined by the propagation medium. Accurate localization and identification are possible if the target is located inside the convex hull of the network. Far-field targets are located at much farther distance relative to the baseline width of the network. For these targets, source localization and range estimation are much more challenging. Due to greater physical distance from the network, signals encounter both increased dispersion and attenuation.

There are two types of cooperative signal processing techniques:

I. Non-coherent
II. Coherent

For non-coherent processing, raw sensor data will be pre-processed at each node to extract a small set of parameters to be forwarded to a central node (CN) for further processing; for coherent processing like blind beam-forming, raw sensor data, after minimal pre-processing, will be tagged with a time stamp and uploaded through the local network to the CN for more intensive computations. Although energy efficiency is the ultimate goal, different approaches can be used depending on what cooperative functions are used.

Non-coherent functions have fairly low data traffic loading; therefore we will focus our effort on improving algorithmic efficiency. On the other hand, since coherent processing generates long data streams, energy efficiency must be achieved by path optimality. For clarity of presentation, we separately discuss coherent and non-coherent processing networks.

V. RELATED WORK

Security issues in ad-hoc networks are similar to those in sensor networks and have been well enumerated in the literature [8, 9], but the defense mechanisms developed for ad-hoc networks are not directly applicable to sensor networks. There are several reasons for why this is so, but they all relate to the differences between sensor and ad-hoc networks enumerated in the previous section.

Some ad-hoc network security mechanisms for authentication and secure routing protocols are based on public key cryptography [8, 10–16]. Public key cryptography is too expensive for sensor nodes. Security protocols for sensors networks must rely exclusively on efficient symmetric key cryptography.

Secure routing protocols for ad-hoc networks based on symmetric key cryptography have been proposed [17]. These protocols are based on source routing or distance vector protocols and are unsuitable for sensor networks. They are too expensive in terms of node state and packet overhead and are designed to find and establish routes between any pair of nodes—a mode of communication not prevalent in sensor networks.

Marti et al. [18] and Buchegger and Boudec [19] consider the problem of minimizing the effect of misbehaving or selfish nodes on routing through punishment, reporting, and holding grudges. These applications of these techniques to sensor networks are promising, but these protocols are vulnerable to blackmailers.

VI. 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 overheard packets. We assume that if the defender can deploy many sensor nodes, then the adversary will likely also be able to deploy a few malicious nodes with similar hardware capabilities as the legitimate nodes.

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.

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.

VII. 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] Y.-C. Hu, A. Perrig, D.B. Johnson, Packet leashes: a defense against wormhole attacks in wireless networks, Proceedings - IEEE INFOCOM DOI:10.1109/INFCOM.2003.1209219 ISBN: 0-7803-7752-4 In proceeding of: INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, Volume: 3.

[2] D. Ganesan, R. Govindan, S. Shenker and D. Estrin, Highly resilient, energy efficient multipath routing in wireless sensor networks, ACM Mobile Comput. and Commun. Review 5(4) (2001) 11–25

[3] G.J. Pottie andW.J. Kaiser,Wireless integrated network sensors, Commun. ACM 43(5) (2000) 51–58

[4] A. Savvides, C.-C. Han and M.B. Strivastava, Dynamic fine-grained localization in ad-hoc networks of sensors, in: ACM Int'l Conf. on Mobile Computing and Networking (MobiCom) (2001) pp. 166–179.

[5] E. Shih, S.-H. Cho, N. Ickes, R. Min, A. Sinha, A. Wang and A. Chandrakasan. Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks, in: ACM Int'l Conf. on Mobile Computing and Networking (MobiCom) (2001) pp. 272–287.

[6] William A. Arbaugh, Dept. of Computer Science, University of Maryland at College Park;waa@cs.umd.edu

[7] K. Sohrabi, On Low Power Wireless Sensor Networks, Ph.D. Dissertation, Department of Electrical Engineering, UCLA, June 2000.

[8] L. Zhou, Z. Haas, Securing ad hoc networks, IEEE Network Magazine 13 (6) (1999) 24–30.

[9] F. Stajano, R.J. Anderson, The resurrecting duckling: security issues for ad-hoc wireless networks, in: Seventh International Security Protocols Workshop, 1999, pp. 172–194.
[10] J. Kong, P. Zerfos, H. Luo, S. Lu, L. Zhang, Providing robust and ubiquitous security support for mobile ad-hoc networks, in: ICNP, 2001, pp. 251–260.
[11] J. Hubaux, L. Buttyan, S. Capkun, The quest for security in mobile ad hoc networks, in: Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC 2001), 2001.
[12] M.G. Zapata, Secure ad-hoc on-demand distance vector (SAODV) routing, IETF MANET Mailing List, Message ID: 3BC17B40.BBF52E09@nokia.com,
Available at ftp://manet.itd.nrl.navy.mil/pub/manet/2001-10.mail, October 8,2001.
[13] J. Binkley, W. Trost, Authenticated ad hoc routing at the link layer for mobile systems, Wireless Networks 7 (2) (2001) 139–145.
[14] H. Luo, P. Zefros, J. Kong, S. Lu, L. Zhang, Self-securing ad hoc wireless networks, in: Seventh IEEE Symposium on Computers and Communications (ISCC 02), 2002.
[15] B. Dahill, B.N. Levine, E. Royer, C. Shields, A secure routing protocol for ad-hoc networks, Tech. Rep. UM-CS-2001-037, Electrical Engineering and Computer Science, University of Michigan, August 2001.
[16] J.Kong,H. Luo,K.Xu,D.L.Gu,M.Gerla, S. Lu,Adaptive security for multilayer ad-hoc networks, Wireless Communications and Mobile Computing 2 (5) (2002) 533–547.
[17] Y.-C. Hu, D.B. Johnson, A. Perrig, SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks, in: Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA2002), 2002, pp. 3–13.
[18] S. Marti, T.J. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in: Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking, 2000, pp. 255–265.
[19] S. Buchegger, J.-Y.L. Boudec, Nodes bearing grudges: towards routing security, fairness, and robustness in mobile ad hoc networks, in: Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing, IEEE Computer Society, Canary Islands, Spain, 2002, pp. 403–410

