Kablosuz Algılayıcı Ağlarında Güvenlik: Kapsamlı Bir Araştırma

Suat ÖZDEMİR

ÖZET

Günümüz dünyasında Kablosuz Algılayıcı Ağları (KAA) izleme ve takip etme gibi birçok aktiviteye yön vermektedir. Bu ağların genelde gözetimsiz ortamlarda kullanılmaları ve kaynakları sınırlı algılayıcılar yüzünden, KAA'lar içerden ve dışardan gelebilecek birçok güvenlik atağına karşı savunmasızdırlar. Güvenlik ataklarına karşı olan savunma zafiyetleri ve KAA'larda taşınan verinin hassasiyeti düşünüldüğünde güvenlik mekanizmalarına çok fazla ihtiyaç vardır. Dahası, KAA'ların kendilerine has özellikleri sebebiyle bu güvenlik mekanizmaları sistem tasarımı aşamasında geliştirilmelidir. Bu çalışmada, KAA'ların güvenlik sorunlarına ait önemli çalışmalar araştırılmış, karşılaşılan engeller ve gereklilikler sunulmuş ve alanda açık olan araştırma konuları gösterilmiştir.

Anahtar Kelimeler: Güvenlik, kablosuz algılayıcı ağları

Wireless Sensor Network Security: A Comprehensive Overview

ABSTRACT

Wireless sensor networks (WSNs) are shaping many activities in today's world such as surveillance and tracking. Due to their unattended nature and resource-constrained sensor nodes, however, WSNs are extremely vulnerable against any kind of internal or external security attacks. Considering these vulnerabilities and sensitivity of the data transmitted on WSNs, there is a tremendous need for security mechanisms. Moreover, because of the unique properties of WSNs, these security mechanisms must be developed during system design process. In this paper, we survey the "state-of-the-art" in WSN security, present the obstacles and requirements, and highlight the open research areas that need to be addressed.

Keywords: Security, wireless sensor networks

1. INTRODUCTION

Wireless Sensor Networks (WSN), composed of hundreds or thousands of inexpensive, low-powered sensing devices with limited computational and communication resources are quickly gaining popularity (1). In a typical WSN, a number of sensor nodes collect application specific information from the environment, and this information is transferred to a central base station, where it is processed, analyzed, and used by the application. An example WSN is shown in Figure 1. These networks offer potentially low cost solutions to array of problems in both military and civilian applications, including battlefield surveillance, target tracking, environmental and health care monitoring, wildfire detection, and traffic regulation. Most of these applications require a certain level of network security. However, due to resource constrained sensor nodes, unattended deployment, and unreliable communication channels, WSNs are extremely vulnerable to any type of internal or external security attacks. In addition, resource constrained sensor nodes prohibit the implementation of traditional computer security techniques. Hence, security solutions of WSNs should be designed by considering unique characteristics of these networks.

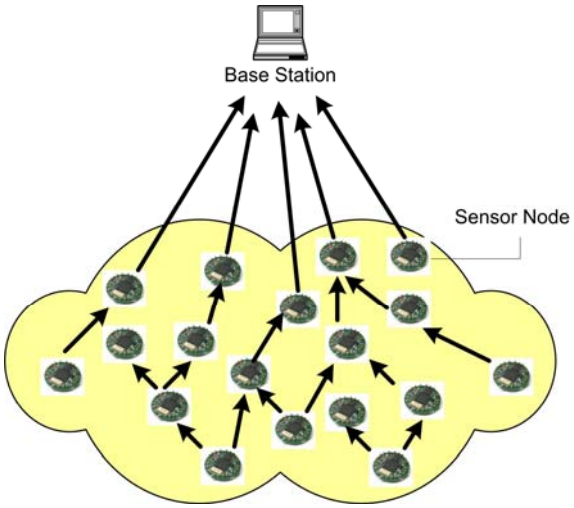

Figure 1. An example of WSN.

Makale 15.08.2007 tarihinde geldi, 18.04.2008 tarihinde yayınlanmak üzere kabul edilmiştir.

S. ÖZDEMİR, Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisligi Bölümü,
Maltepe, Ankara, 06570, TÜRKİYE
suatozdemir@gazi.edu.tr

Digital Object Identifier 10.2339/2008.11.3.207-214

The necessity of securing WSNs under strict limitations motivated researchers to incorporate security in all aspects of WSNs from the beginning of the system design process. However, there are still security issues that require further research. In this paper, security attacks against WSNs and their countermeasures are identified. Given WSN characteristics and security attacks, open research areas are presented. The rest of the paper organized as follows. Section 2 presents the unique characteristics of WSNs whereas the security requirements of WSNs are given in Section 3. Security attacks against WSNs along with their corresponding defense mechanisms are presented in Section 4. Section 5 discuses the open research areas. Finally, concluding remarks are given in Section 6.

2. CHARACTERISTIC OF WIRELESS SENSOR NETWORKS

The aforementioned resource constrains of sensor nodes and the large scale of WSNs introduce a new set of research issues and challenges that previous research did not need to address. In what follows, we summarize the characteristics of WSNs that distinguish them from traditional ad hoc networks.

Large scale

Typical application areas of WSNs (e.g., battlefields) require a large geographic coverage. At the same time, a high node density is required to work against the high failure rate of sensor nodes, the low confidence in individual sensor readings, and the limited communication range of sensor nodes. Due to such reasons, WSNs are expected to scale up to thousands of nodes.

Constrained resource

Because of the low-cost deployment requirement of WSNs (1), sensor nodes have a simple hardware which severely limits the processing and communication ability of sensor networks. For example, one common sensor type (TelosB) has a 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage (2). In addition, once the network is deployed, the batteries of sensor nodes cannot be easily replaced or recharged. Hence the lifetime of individual sensor nodes and the entire sensor network depends on battery charge of sensor nodes. Low processing speed, limited memory, constrained energy supply, and bandwidth make it a challenge to design any protocol intended for sensor networks.

Redundancy

The highly unpredictable nature of WSNs and short communication range of sensor nodes necessitate a high node redundancy. Sensor nodes are normally deployed with a high degree of connectivity to cope with sensor node failures. With such redundancy, the failure of a single node has a negligible impact on overall capacity of the sensor networks. On the other hand, redundancy increases the amount of data to be transmitted from sensor nodes to base station which greatly reduces the network lifetime. Therefore, high data redundancy in WSNs has to be eliminated by data aggregation protocols.

Security sensitive

Many WSN applications, such as surveillance, military tracking or biomedicine, are highly security sensitive. Due to constrained resources, it is not possible to deal with all possible security issues, yet WSNs are vulnerable to node capture attack which does not exist in traditional networks. Therefore, security solutions of sensor networks must consider the limitations of sensor nodes and be resilient against node capture attacks.

Data centric processing

Data centric processing is an intrinsic characteristic of WSNs. The IDs of the sensor nodes are of no interests to the applications therefore naming schemes in sensor networks are usually data oriented. For example, an environmental monitoring system requests the temperature readings through queries such as "collect temperature readings in the region area bound by the rectangle (x_1, y_1, x_2, y_2)", instead of queries such as "collect temperature readings from a set of nodes with the sensor node IDs x, y and z."

High unpredictability

Sensor node failures are common due to the large number of sensor nodes, low-cost sensor hardware, climate conditions and hostile environment. The wireless medium shared by densely deployed sensor nodes is subject to heavy congestion and jamming. High bit error ratio, low bandwidth and asymmetric channel make the communication highly unpredictable. Such unpredictability usually prevents off-line design of system parameters. Online monitoring and feedback control are required to provide a certain degree of quality-of-service under such situations.

Real-time constraints

Since WSNs deal with the real world processes, it is often necessary for communication to meet real-time constraints. In border surveillance systems, for example, communication delays within sensing and actuating loops directly affect the quality of target tracking. Due to the nature of the wireless communication and unpredictable traffic pattern, it is infeasible to guarantee hard real-time constrains, however, research that provides probabilistic guarantee for timing constraints is quite achievable and essential.

3. SECURITY REQUIREMENTS OF WIRELESS SENSOR NETWORKS

Security is an important issue for WSNs due to unique requirements of its own as discussed in the previous section. This section presents the security requirements which are suited solely to WSNs. Some of

these requirements share some commonalities with typical computer networks; however they are presented from the WSN point of view.

Data confidentiality

In WSNs confidentiality ensures that secrecy of sensed data is never disclosed to unauthorized parties and it is the most important issue in mission critical applications. Authors of (3) and (4) state that a sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive. Furthermore, in many applications sensor nodes transfer highly sensitive data, e.g., key distribution; hence it is extremely important to build a secure channel in a WSN. Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks. In addition to these, routing information must also remain confidential in certain cases as malicious nodes can use this information to degrade the network's performance. 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.

Data integrity

Data confidentiality may guarantee that intruders cannot obtain the data, however it does not protect data from being altered. Data integrity guarantees that a message being transferred is never corrupted. A malicious node may just corrupt messages to prevent network from functioning properly. In fact, data may be altered without the presence of an intruder due to unreliable communication channels. Hence message authentication codes or cyclic codes should be used to prevent data integrity.

Source authentication

Since WSNs use a shared wireless medium, sensor nodes need authentication mechanisms to detect maliciously injected or spoofed packets. Source authentication enables a sensor node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. If only two nodes are communicating, authentication can be provided by symmetric key cryptography. The sender and the receiver share a secret key to compute the message authentication code (MAC) for all transmitted data. However, for broadcast authentication more complex techniques are required. Perrig *et al*. propose secure broadcast protocol, called µTESLA (3) which achieves asymmetric cryptography by delaying the disclosure of the symmetric keys. µTESLA is based on hashed key chains that must be unicast to each sensor node before authentication of broadcast messages can begin. Broadcasted messages are disclosed by receiver until the sender will disclose the secret key. After disclosure, the receiver can authenticate the packet, provided that the packet was received before the key was disclosed. Unicast deficiency of µTESLA scheme is remedied in (5, 6) by broadcasting the key chain commitments.

Availability

Availability guarantees the survivability of network services despite denial-of-service attacks. A DoS attack could be launched at any layer of a WSN and may disable the victim node(s) permanently. In addition to denial-of-service attacks, excessive communication or computation may exhaust battery charge of a sensor node. Consequences of availability loss may be catastrophic. For example, in a battlefield surveillance application, if the availability of some sensor nodes cannot be provided, this may open a back door for enemy invasion. WSNs are deployed with high node redundancy to tolerate such availability losses.

Localization

For WSNs, the vitality of a sensor node's location is a critical feature because a WSN's utility relies on its ability to accurately locate each sensor in the network. In any WSN application, the location information of nodes plays a vital role to identify the location of an event of interest. For instance, the location of a fire is of critical importance for deploying fire rescue teams. Moreover, location information is used in many system functionalities, such as location-based information querying (7), geographical routing (8, 9, 10), and network coverage checking (11). Hence the correctness of location information significantly affects the performance of these protocols.

Table 1. Attacks that are covered in this paper.

Denial-of-Service Attacks	Jamming Collision generation Desynchronization Selective forwarding Misdirection Sinkhole generation Wormhole generation Flooding
Sybil Attacks	Identity duplication
Attacks on data integrity	False data injection to forwarded and aggregated data
Attacks on Data Confidentiality	Pairwise key compromise
Traffic Analysis Attacks	Base station and data aggregator identification
Physical Attacks	Node capturing

4. ATTACKS AND COUNTERMEASURES

As stated previously, WSNs are particularly vulnerable to number of attack types which can be mounted in a variety of ways. While majority of these attacks aim to degrade the network's performance, others target data confidentiality, data integrity, physical security of nodes, and so on. This section presents the most important security attacks in WSNs and provides

their countermeasures. Table 1 summarizes the attacks that are covered in this section.

4.1 Denial-of-Service Attacks

A Denial-of-Service (DoS) attack is defined as any event that diminishes or eliminates a network's capacity to perform its expected function (12). Mounting a DoS attack in WSNs is relatively easy because of the lack of physical security of sensor nodes. Once a sensor node is compromised, an intruder is able to do anything to prevent the network perform properly. In addition to intruders, hardware failures, software bugs, resource exhaustion, environmental conditions, or any complicated interaction between these factors can cause a DoS. Moreover, it is a non-trivial task to determine if a fault or collection of faults is the result of an intentional DoS attack. Hence, DoS attacks have well studied in the WSN literature (12-16).

The simplest form of DoS attacks is to jam sensor nodes by transmitting radio signals that interfere with the radio frequencies being used by the sensor network (45). There are two types of jamming attacks, namely constant jamming in which the intruder jams the whole network constantly and intermittent jamming in which the intruder jams the network at irregular intervals. The simplest defense against jamming is to employ various forms of spread-spectrum communication (36). To by pass frequency hoppers, intruders must be able either to follow the precise hopping sequence or to jam a wide section of the band. However, frequency (or code) hopping techniques require greater design complexity and more power and therefore may not be suitable to low cost, low-power sensor nodes (12). For sensor nodes, the effective way of defending against jamming attacks is to lower their energy consumption during the jamming attack. This is achieved by staying in sleep mode as much as possible and periodically checking whether the jamming has ended.

Link layer DoS attacks can be performed by constantly or intermittently transferring packets to generate collisions in wireless medium access, thereby requiring sensor nodes to retransmit their packets. Through link layer DoS attacks, intruders may deplete a sensor node's power supply by forcing too many retransmissions. Another link layer attack is desynchronization where an intruder tries to disrupt the connection between two nodes by forging the sequence numbers of the transmitted messages. Due to desynchronized message sequence numbers, two nodes waste their energy to recover message synchronization. Against link layer DoS attacks, sensor nodes can use collision detection to identify malicious collisions or use error-correcting codes to detect corrupted messages.

At routing layer, intruders may perform DoS attack in the form of selective forwarding. In selective forwarding attack, malicious nodes may arbitrarily neglect to forward certain messages and simply drop them, ensuring that they are not propagated any further. A naïve way of mounting selective forwarding attack for a malicious sensor node is to refuse forwarding every packet it receives. However, such a node may be considered as failed by its neighbors and neighboring nodes decide to seek another route. A more sophisticated form of this attack is when a malicious node selectively forwards packets instead of dropping all of them. This attack is hard to detect because due to in network processing neighboring nodes cannot distinguish if a packet is dropped or eliminated. The dynamic source routing (DSR) (17) is especially vulnerable to this attack as all the routes are cached in the network. If a malicious node is on one of the routes, it may degrade the network's performance. Sending redundant data packets over multiple data paths can reduce the effect of this attack by requiring intruder to compromise a sensor node on each path (12, 18).

Misdirection, sinkhole and wormhole are other DoS attack types that can be launched from routing layer. In misdirection attacks, malicious nodes forward data packets along wrong paths, perhaps by fabricating malicious route advertisements (18). This DoS attack may prevent or delay sensor data to reach its destination resulting in draining the battery power of sensor nodes on the path. A malicious node can also aim to defuse an arbitrary victim node in the network by misdirecting many traffic flows to victim node's direction. Sensor nodes can use encrypted routing headers to defend against this attack.

In sinkhole attacks, intruder's aim is to channel all the traffic from a particular area towards a malicious node. This creates a sinkhole; the receiver malicious node in the sinkhole can drop the packets resulting in data loss in the network. As shown in Figure 2, in order to perform sinkhole attack, a malicious node could broadcast an advertisement for a high quality path to the base station. However, it forwards all the received traffic to the sinkhole instead of the base station. The quality of these advertised paths must be verified with end-to-end acknowledgements such as checking the latency values of the paths (18).

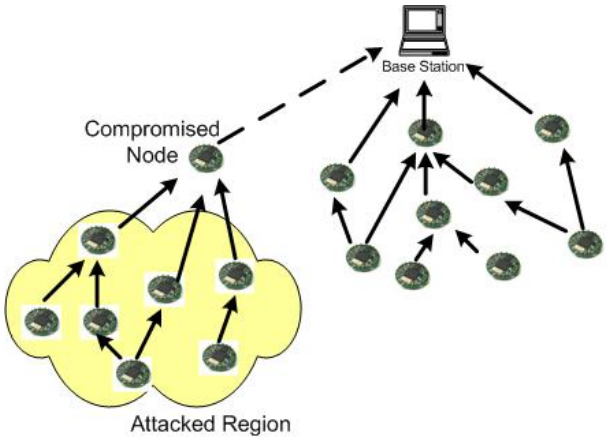

Figure 2. Sinkhole attack

Wormholes can be used to mount sinkhole attacks in which there are two powerful malicious nodes (e.g., laptop) (18). The first malicious node is located close to base station and the other one is located far away from base station and establishes a low latency channel with the first malicious node. Figure 3 illustrates an example wormhole attack setup. The malicious node located far away from base station advertises the low latency link to base station, and actually send the received packets to other malicious node. At the other end of the low latency channel, second malicious node can drop or selectively forward the packets. Wormhole attacks cannot be detected using end-to-end acknowledgements based on latency information as there is really a low latency channel towards base station (18). The simplest defense mechanism against wormhole attacks is to let only authorized nodes to exchange routing information. However, if the authorized nodes are compromised, this prevention mechanism is invalidated. Sensor nodes can also monitor their neighbors to ensure that they observe proper routing behavior. For example, the watchdog mechanism introduced in (37), the node relays a message to the next hop and then acts as a watchdog that verifies the next-hop transmission of the same packet.

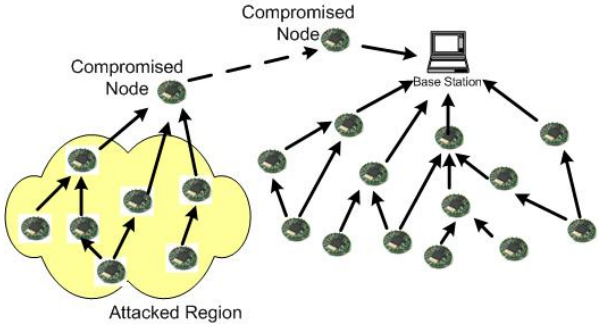

Figure 3. Wormhole attack

Flooding attacks are realized in transport layer by sending to many control messages, e.g., connection request, to a sensor node so that the node allocates its all resources to reply those control messages. The basic solution to this attack is limiting the number of connection requests per unit time. However, this naïve solution also limits the legitimate nodes and may result in data lose. A more sophisticated solution is to employ challenge-response or client puzzles where nodes that wish to establish a connection must solve a challenge or a puzzle before making the connection request (12). Hence, an intruder who wants to flood a node must allocate much more computational resources.

4.2 Sybil Attacks

In Sybil attack, a single malicious node presents multiple identities to other nodes in the network (19, 20). Sybil attack can significantly degrade the performance of many protocols such as data aggregation, multipath routing, or topology maintenance protocol. For example, Sybil attack poses significant threat to data aggregation protocols. Aggregated data cannot be affected by a small number of malicious nodes reporting incorrect sensor readings. However, using Sybil attack, one malicious node may be able to significantly change the aggregated data by contributing to the aggregation many times. Especially, if Sybil nodes are cluster-heads or aggregators then the effect of this attack may be catastrophic resulting in completely altered aggregated data. Sybil attack also presents a threat to geographic routing protocols (21). Location aware routing often requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets, by using Sybil attack a malicious node can pretend to "be in more than one place at one time" and routes all sensor data towards itself. Sybil attack can be defended using various techniques such as random key predistribution protocols (20). In order to use random key distribution techniques for defending against the Sybil attacks, each node ID must be associated with the keys assigned to that node and a key validation must be performed. Additionally, location based key establishment protocols (38, 39) and resource testing protocols (20) can also be used against Sybil attack.

4.3 Attacks on data integrity

Compromised sensor nodes can forge the integrity of sensor data by injecting false data or change forwarded data during forwarding. It is highly desirable for sensor nodes to detect and drop such forged or false data as soon as possible in order to avoid depleting their limited resources such as battery power and bandwidth. By injecting false data, compromised sensor nodes can distort data integrity, cause false alarms, and reduce the limited battery, computational and communication resources of sensor nodes. Standard data authentication protocols cannot prevent false data injection attacks if there is more than one compromised node in the network (22). Hence, data authentication protocols based on collaborative data authentication must be employed against false data injection attacks (22-25). Moreover, false data injection attacks can be performed during data aggregation as well. In fact, it is a challenging task to detect false data injections during data aggregation because data aggregation results in data alterations. Therefore, to determine whether any data alteration is due to data aggregation or false data injection, false data detection protocols must be designed with data aggregation protocols (40).

4.4 Attacks on Data Confidentiality

The information transmitted on WSNs may be private. For example, in a military application, it is clear that enemies should not have access to the collected information. Standard cryptographic techniques can protect the secrecy of communication links from outsider attacks such as eavesdropping. Two sensor nodes that need to set up a private communication link

must share a pairwise key. Public key cryptography is a well accepted method for key establishment but because of the high computational cost it is not feasible for WSNs. Hence pairwise keys need to be distributed to sensor nodes. The simplest solution to key distribution problem is to use a global key stored on each sensor node prior to deployment. But, this approach is particularly vulnerable to node capture attacks because if an intruder captures a single node, then all communication links will be compromised. Recently, a number of random key predistribution techniques are proposed (26-30). The basic idea behind these techniques is to select a random pool of keys from the key space and then distribute a random subset of keys from the key pool to each sensor node before deployment. Any two sensor nodes that are able to find one common key within their respective key subsets use that key as their shared secret to initiate secure communication. However, further research is necessary to improve these techniques in terms of scalability, resilience to node compromise, memory requirements, and communication overhead.

4.5 Traffic Analysis Attacks

Data flow pattern of WSNs is usually many to one because many low-power sensors send their responses to queries broadcasted by a powerful base station. Also, for in network processing, sensor data are collected by intermediate sensor nodes, called data aggregators. To render the network's operation, intruders aim to disable base station and data aggregators. Therefore, in many applications of WSNs, identity of the nodes sending/receiving data to/from a data aggregator or the base station is extremely sensitive information. To identify aggregators and the base station, intruders perform traffic analysis attacks. Encrypting data may not be the suitable a solution because in (31) two attack types are presented to identify the base station in a network that uses encrypted data packets. Instead of data encryption, design and deployment of effective anonymity solutions is essential to solve the problem of traffic analysis in WSNs (32).

4.6 Physical Attacks

Sensor networks typically operate in hostile outdoor environments. Moreover, due to low cost requirement of WSNs, sensor nodes cannot be tamper proof. Hence, one of possible attacks on WSNs is called node capture in which an intruder can gain full control over some sensor nodes through direct physical access (33). Node capture attack is easy to perform. For example, in a recent study (35) the time required to capture a MICA2 mote (2) is shown to be around one minute. Unlike many other attacks mentioned in this paper, physical attacks may destroy sensor nodes permanently, so the damages are irreversible. As a result of node capturing attacks, intruders can extract cryptographic keys, tamper with the hardware, reprogram the code in the sensor nodes, or replace them with malicious sensor nodes under the control of the intruder (34). In (41) code attestation technique that validates the code running on each sensor node is suggested to detect compromised nodes.

5. OPEN RESEARCH AREAS

Although considerable attention had been paid to WSN security, there are still some issues need to be addressed. Battery energy is the main resource to protect in current WSNs. The security protocols proposed so far either aim to optimize either for a high level of security or for a low energy utilization (43, 44). To achieve high security and low energy consumption, energy efficient cryptographic functions must be developed for WSNs. Especially, more research on low power public key cryptography is needed to solve the key establishment problem. Random key predistribution protocols must also be improved in terms of scalability, resilience to node compromise, memory requirements, and communication overhead (41). As noted in previous sections, coping with compromised nodes is the most difficult challenge of WSN security. In (41) Shi and Perrig state that, to address compromised node problem, a promising direction is to use code attestation that validates the code running on each sensor node. Since the code running on a malicious node must be different from that on a legitimate node, malicious nodes can be detected by verifying their memory content. Software or hardware based code attestation is an open area for WSN security researchers. Another issue that needs to be addressed is that malicious node detection and their revocation from the network. Current research on malicious node detection is based on distributed voting systems which are also susceptible to malicious nodes. For example in these systems, malicious nodes can pretend to be a victim to make a legitimate node look malicious. Therefore, further research is needed to develop distributed voting systems or reputation schemes that cannot be affected by compromised nodes. There are also some new applications which may cause security problems. For example, mobile agents introduced in (42) provide an efficient collaborative processing mechanism. However, its security is not fully evaluated. One problem with mobile agents is that any intruder is able to inject a malicious agent inside a node because of the lack of physical security of sensor nodes. Hence, further investigation is required to provide secure mobile agents to WSNs.

6. CONCLUSION

Security concerns are still the biggest obstacle to the impending widespread deployment of WSNs that will soon play an important role in our daily life. Therefore, security in WSNs is a popular field of research that is growing rapidly. Nevertheless, there is still room for more improvements in this area. This paper summarized WSN security by describing unique properties of WSNs, their security requirements, and

attacks against them. The open research issues such as compromised node detection or implementation of low power public key primitives are also identified. From the security point of view, we see that WSNs are not ready to take over critical missions yet. However, it is expected that improvements in WSN security will open new application areas for these networks.

7. REFERENCES

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., and Cayirci, E., A survey on sensor networks, IEEE Communications Magazine, 40(8), 102-114, 2002.
2. Crossbow Technologies, http://www.xbow.com, 2007.
3. Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., and Culler, D. E. Spins: security protocols for sensor Networks, Wireless Networking, 8(5), 521–534, 2002.
4. Carman, D. W., Krus, P. S., and Matt, B. J., Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.
5. Liu, D. and Ning, P., Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks, 10th Annual Network and Distributed System Security Symposium, San Diego, USA, 263–276, 2003.
6. Liu, D. and Ning, P., Multilevel μTESLA: Broadcast authentication for distributed sensor networks, Trans. on Embedded Computing Systems, 3(4), 800–836, 2004.
7. Gupta, H., Das, S. R., and Gu, Q., Connected Sensor Cover: Self-Organization of Sensor Networks for Efficient Query Execution, MobiHoc, Maryland, USA, 189-200, 2003.
8. Ko, Y. and Vaidya, N. H., Location-aided routing (LAR) in mobile ad hoc Networks, Wireless Networks, 6, 321-324, 2000.
9. Karp, B. and Kung, H. T., Greedy Perimeter Stateless Routing for Wireless Sensor Networks, MobiCom'00, Boston, USA, 243-254, 2000.
10. Mauve, M., Widmer, J., and Hartenstein, H., A Survey on Position-Based Routing in Mobile Ad Hoc Networks, IEEE Network Magazine, 30-39, 2001.
11. Yan, T., He, T., and Stankovic, J.A., Differentiated Surveillance Service for Sensor Networks, First ACM Conference on Embedded Networked Sensor Systems (SenSys '03), Los Angeles, USA, 51-62, 2003.
12. Wood, A.D. and Stankovic, J. A., Denial of service in sensor networks. Computer, 35(10), 54–62, 2002.
13. Zhou, L. and Haas, Z., Securing ad hoc networks, IEEE Network Magazine, 13(6), 24-30, 1999.
14. Hu, Y-C., Perrig, A. and Johnson, D.B., Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks, Wireless Networks Journal, 11(1), 21-38, 2005.
15. Zapata, M.G. and Asokan, N., Securing ad hoc routing protocols. 3rd ACM Workshop on Wireless Security, Atlanta, USA, 1-10, 2002.
16. Basagni, S., Herrin, K., Bruschi, D., and Rosti, E., Secure pebblenets, 2nd ACM international Symposium on Mobile Ad Hoc Networking & Computing, Long Beach, USA, 156-163, 2001.
17. Johnson, D.B. and Maltz, D.A., Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing, T. Imielinski and H. Korth, eds., Kluwer Academic, vol. 353, 153-181, 1996.
18. Karlof, C. and Wagner, D., Secure routing in wireless sensor networks: Attacks and countermeasures, Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, vol. 1, no. 2-3, 293-315, 2003.
19. Douceur, J. R., The Sybil Attack, Lecture Notes In Computer Science, P. Druschel, M. F. Kaashoek, and A. I. Rowstron, eds. vol. 2429, 251-260, 2002.
20. Newsome, J., Shi, E., Song, D., and Perrig, A., The Sybil Attack in Sensor Networks: Analysis & Defenses, Third international symposium on Information processing in sensor networks, Berkeley, CA, USA, 259-269, 2004.
21. Yu, Y., Govindan, R., and Estrin, D., Geographical and energy aware routing: a recursive data dissemination protocol for wireless sensor networks, Tech. Rep. UCLA/CSD-TR-01-0023, Computer Science Department, University of California at Los Angeles, 2001.
22. Ye, F., Luo, H., Lu, S. and Zhang, L., Statistical En-route Detection and Filtering of Injected False Data in Sensor Networks, IEEE INFOCOM 2004, Hong Kong, China, 2446-2457, 2004.
23. Zhu, S., Setia, S., Jajodia, S., and Ning, P., An Interleaved Hop-by-Hop Authentication Scheme for Filtering False Data in Sensor Networks, IEEE Symposium on Security and Privacy, Oakland, CA, 259-271, 2004.
24. Yang, H. and Lu, S., Commutative Cipher Based En-Route Filtering in Wireless Sensor Networks, IEEE VTC Fall 2004, Los Angeles, CA, 1223- 1227, 2004.
25. Yu, Z. and Guan, Y., A Dynamic En-route Scheme for Filtering False Data in Wireless Sensor Networks, IEEE INFOCOM 2006, Barcelona, Spain, 1-12, 2006.
26. Liu D. and Ning, P., Establishing pairwise keys in distributed sensor networks, 10th ACM Conference on Computer and Communications Security, Washingtion, USA, 52-61, 2003.
27. Du, W., Deng, J. and Varshney, P. K., A pairwise key pre-distribution scheme for wireless sensor networks, 10th ACM Conference on Computer and Communications Security, Washingtion, USA, 42-51, 2003.
28. Eschenauer, L. and Gligor, V. D., A key-management scheme for distributed sensor networks, 9th ACM conference on Computer and communications security, Washington, DC, 41-47, 2002.
29. Du, W., Deng, J., Han, Y. S., Chen, S., and Varshney, P. K., A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge, IEEE INFOCOM'04, Hongkong, China, 597-608, 2004.
30. Chan, H., Perrig, A., and Song, D., Random key predistribution schemes for sensor networks, IEEE Symposium on Security and Privacy, Berkeley, California, 197-213, 2003.
31. Deng, J., Han, R., and Mishra, S., Countermeasuers against traffic analysis in wireless sensor networks, Technical Report CU-CS-987-04, University of Colorado at Boulder, 2004.

32. Misra, S. and Xue, G., Efficient anonymity schemes for clustered wireless sensor networks, Int. Journal of Sensor Networks (IJSNET), vol. 1, 50-63, 2006.

33. Becher, A., Benenson, Z., and Dornseif, M., Tampering with motes: Real-world physical attacks on wireless sensor networks, 3rd International Conference on Security in Pervasive Computing (SPC), York, UK, 2006.

34. Wang, X., Gu, W., Chellappan, S., Xuan, D., and Laii, T.H., Search-based physical attacks in sensor networks: Modeling and defense. Technical report, Dept. of Computer Science and Engineering, The Ohio-State University, 2005.

35. Hartung, C., Balasalle, J. and Han, R., Node compromise in sensor networks: The need for secure systems. Technical Report Technical Report, CU-CS-988- 04, Department of Computer Science, University of Colorado at Boulder, 2004.

36. Anderson, R., Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley Computer Publishing, New York, 326-331, 2001.

37. Marti, K. L. S., Giuli, T. J. and Baker M., Mitigating routing misbehavior in mobile ad hoc networks, 6th Intl. Conference on Mobile Computing and Networking, August 6-11, Boston, Massachusetts, 255-265, 2000.

38. Liu, D. and Ning, P., Location-based pairwise key establishments for static sensor networks, 1st ACM workshop on Security of ad hoc and sensor networks, Fairfax, Virginia, 72-82, 2003.

39. Zhang, Y., Liu, W., Lou, W., and Fang, Y., Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks, JSAC, Vol. 24, Number 2, 247-260, 2006.

40. Çam, H., and Özdemir, S., False Data Detection and Secure Data Aggregation in Wireless Sensor Networks, Security in Distributed, Grid, Mobile and Pervasive Computing", Auerbach Publications, CRC Press, 2007, ISBN: 9780849379215.

41. Shi, E., Perrig, A., Designing secure sensor networks, Wireles Communications, IEEE , vol.11, no.6, 38-43, 2004.

42. Qi, H., Xu, Y., Wang, X., Mobile-agent-based collaborative signal and information processing in sensor networks, Proceedings of the IEEE, vol.91, no.8, 1172-1183, 2003.

43. Karlof, C., Sastry, N., and Wagner, D., TinySec: a link layer security architecture for wireless sensor networks, 2nd international Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, 162-175, 2004.

44. Luk, M., Mezzour, G., Perrig, A., and Gligor, V., MiniSec: a secure sensor network communication architecture. 6th international Conference on information Processing in Sensor Networks, Cambridge, Massachusetts, USA, 479-488, 2007.

45. Wood, J., Stankovic, A., and Son, S.H., Jam: A jammed-area mapping service for sensor networks, 24th IEEE Real-time Systems Symposium (RTSS'03), Cancun, Mexico, 286-297, 2003.