AENSI Journals

Advances in Environmental Biology

ISSN-1995-0756 EISSN-1998-1066

Journal home page: http://www.aensiweb.com/AEB/

Attacks and Secure Strategies in Wireless Sensor Networks

Siavash Dehdar, Ali Haroonabadi and Seyyed Javad Mir Abedini

Department of computer, Kish International Branch, Islamic Azad University, Kish Island, Iran

ARTICLE INFO

Article history:
Received 13 June 2014
Received in revised form 22 July 2014
Accepted 10 September 2014
Available online 21 September 2014

Keywords:
Security, Protocol, Threat, Attack, Wireless Sensor Network, Protection

ABSTRACT

Today, the security of wireless sensor networks is vital and inevitable for using them in military, telecommunication, and industrial industries by increasing the demand. Identifying the threats and attacks on the network and the protection ways against attacks have a significant effect on the efficiency of wireless sensor networks since the wireless sensor networks expose to extensive attacks. In this article, the most prominent attack on the sensor network will be considered and the ideas and strategies which are used to confront with these attacks will be described. Since the attacks can enter into the sensor networks through telecommunication routes, the role of standard telecommunication protocols in wireless sensor networks and evaluating the security of them against attacks will be considered in this article and at last, the best secure protocol will be recognized and the bases will be made securely to create other protocols.

To Cite This Article: Siavash Dehdar, Ali Haroonabadi and Seyyed Javad Mir Abedini., Attacks and Secure Strategies in Wireless Sensor Networks. ***Adv. Environ. Biol., 8(12),*** *743-749, 2014*

INTRODUCTION

A wireless sensor network has been made of hundreds of loops of sensors in large measurement and most of them have been spread in a vast area. Sensor loops are small and they have limit ability in calculations and telecommunications which are fed by batteries. These small sensor loops are prepared to be attacked by different kinds of attacks and it is not practical to control and protect completely each one of sensor loops against physical or logical attacks for a sensor network in large measurement. Attacks in wireless sensor networks can be categorized on the basis of attackers' ability such as the sensor level's attackers and laptop level's attackers.

Laptop level:

A laptop level's attacker delivers a radio frequency into the wireless sensor network by its laptop and starts to damage and gradually causes to damage more than an attacker which attacks to the sensor level because it has better energy supply and also has more ability in calculations and telecommunications with a sensor loop. The secure strategies are divided into the three groups completely against attacks: the prevention strategies of attack, the discovery of attack, and the reactional actions [1].

The preventive measures which are called recommendation, too, can prevent from attacking and or reduce the attacks. Researchers try to use codification for identifying and confirming the information, integrating, and ensuring the data for this strategy. Discovery of attack is difficult in wireless sensor networks because it is impossible to identify the attack simply by damaging in the network.

The reactional actions appear in several forms:

At first, they order to the all loops of the network simply and disconnect their communications in a period of time and make the network damage. In another case, the network does its main work and the attacker eliminates all trace of its existence, but it handles everything gradually with spreading completely in all over the network. In more complex cases, the reactional actions can change the secure level and or make impossible the spread in the network.

Implementing the secure strategies is complex which needs scientific calculations, consuming the memory and energy resources. The main problem in wireless sensor network [WSN] is that the security is not much to be considered, so attackers can access to the various parts of the network simply and make attacks in these networks which are not permanent in other kinds of networks.

Corresponding Author: Siavash Dehdar, Department of computer, Kish International Branch, Islamic Azad University, Kish Island, Iran
E-mail: Siavash_ Dehdar@yahoo.com

Then, identifying the threats and attacks on the network and the protection ideas against attacks can have significant effect on the efficiency of wireless sensor networks. The communication protocols remove all obstacles for more attacks, so the choice of secure telecommunication protocols has an important role in security of sensor network.

In the rest of this article, the existing threats will be described in sensor network, then the attacks on the sensor network will be described and some ideas will be presented for protecting against attacks. In final section, the telecommunication protocols of sensor network and the ways of attacking to them will be described.

1) *Threats:*

The wireless sensor networks are more susceptible than other wireless networks. The attacks which are entered into the networks are divided into two external and or internal categories. External attacks are in the laptop level group and they are not slight attackers of the network but also overhear inactively in network telecommunications that this work reduces the security of the information. The external attacks in active state produce disorders by creating pauses in network such as noise attacks and or changing the delivered packages and or entering in correct information packages in the network. Another category, the internal attacks can produce damaging codes on the loops of sensor network and reduce the security of sensor keys and disrupt the telecommunications of each loops [2].

A foreigner attacker does not access to the most confidential parts in sensor network, while an internal attacker can have some parts of key and attract the trust of other loops to affect more efficiently. Identifying internal attacks and defense against it is more difficult than external attacks by far [3].

Researches try to find mechanisms to protect the ability of the access of data, complete and integrate the information, validate and secure the data against threats.

The secure threats can damage the physical layer, linking layer [MAC], network layer, transition layer, and applied layer [4].

In sequel, the most fundamental attack in wireless sensor network will be considered and strategies to confront with them will be described and secure standards of wireless sensor networks and their weak and strong points will be declared.

2) *Attacks:*

Attacks are divided into two aggressive and non-aggressive categories. Non-aggressive attacks can affect on the frequency, the time of sending the data and essential ability and energy to transfer data.
Aggressive attacks are the most important attacks which will be described elaborately in sequel.

1-3. Denial of Service [DOS]:

One standard attack on one wireless sensor network is the denial of one or a series of loops. Denial is the transition of one radio signal which disrupts radio frequency used by sensor network. The denial of one network is delivered into two categories: fixed denial and alternative denial. Fixed denial consists of disrupting the whole network and no messages can be delivered and received. If denial continues alternatively, loops can exchange their messages in different periods of time. This sensitivity of the messages to the time can have disadvantageous effect on the sensor network. The attacks of Denial of Service [DOS] can disrupt in telecommunication protocols such as ZigBee or 802.15.4 by transition of message.

Messages also cause disruption in the network in tracing layer by not tracing. Each neighbor which traces through the loop cannot communicate and deliver messages.

1-1-3. Protection Against attacks of DOS:

One strategy in protection of disruptive attacks of identifying the disruptive sensor network and the choice of suitable route is not accessible.

In this strategy, loops around the disruptive area inform their neighboring loops and system can surround disruptive area easily. Another way is putting new algorithms in transitional route of information from source to the destination so that they can discover the attacks. Another solution, decrease in delivery by making small the size of frames in MAC layers.

2-3. Sybil Attack:

In this attack, one destructive loop has various identities. These attacks affect on tracing of algorithms, the accumulation of data, voting, giving resources and identifying incorrect behavior. The destructive loop takes the identity of such loop and shows different routes of tracing a loop.

1-2-3. Protection against Sybil Attack:

There should be a mechanism against Sybil attack to defend which confirms an obvious identity is an identity that one physical obvious loop has. There are two ways of confirming the identity against Sybil attack.

Direct confirm that reliable loop controls the identity directly and in indirect confirm of one secure loop are considered for guaranteeing the credit of connected loop [5].

3-3. Physical Attack:

Sensor networks usually operate in the space of foreigner attacker. In such areas, sensors which have been implemented by unnatural and explained nature are exposed to physical attacks. Physical attacks destroy sensors completely forever, so the effect of this attack is permanent. For instance, attackers can find main codes, change the orbits, change the programming of sensor or produce sensors under the control of attackers alternatively.

1-3-3. Protection against Physical Attack:

Physical attacks are serious dangers for wireless sensor networks due to environmental unconsidered features and limited resources. Maybe, sensor loops have physical hardware that protection is increased against attacks by it. For example, one defense such as resistant sensors against manipulation is for protection against sensor manipulation that it keeps the information on sensor out of the reach of attacks. Another method is creating hardware and software out of sensors for tracking the attack.

Another suitable way for protecting the sensors from physical attacks is a way which finishes automatically. In this case, when a sensor identifies an attack, it destroys itself with all keys and data.

4-3. Attack on the Space of Private Limits:

Wireless sensor networks produce abundant volume of data for accessing from long distant; therefore, attackers do not need physical presence. They can acquire information by methods with low risk and unknowingly. Accessing from long distant let attackers consider various areas simultaneously. The most popular attack to the private space is overhearing. The attacker can be aware of the materials of telecommunications easily by listening to the information. When the volume traffic of information is transferred to the network, overhearing can find all its intended information.

Another kind of attack is analyzing the traffic of wireless sensor network. Sensor network is connected with several main strong and fortified stations. The traffic attack uses this idea that loops around the main station tend to deliver packages more than farther loops.

Because of this, the traffic attack can reach the main base and destroys it by identifying the situation of these loops. When an attacker wants to make a network useless, it is enough to destroy the main base [6].

In another kind of attack, attackers enter their codes into the network secretly and or force destructive loops to hide in the sensor network. After that these loops can introduce themselves as usual loops and attract packages. Then, they deliver packages to the false address, for example, they deliver a package to the loops which manage a private space.

1-4-3. Protection against Attacks to the Space of Private Limits:

There are techniques for protecting against these kinds of attacks

Unknown Mechanisms:

When they have exact information from the situation, they recognize users and or track them to attack them. This is a threat to the private limits that unknown mechanisms make data free from information before the information would be released. Of course, being completely unknown is a big problem that causes the situation of loop is not recognized in the network, so it is essential to consider exactly between being unknown and the need to public information.

Decentralized Sensitive Data:

The main idea of this method is the distribution studied situational data through a productive tree [Spanning] that no separate loops have a complete vision to the main data.

Secure Telecommunication Channel:

It can be prevented from overhearing the active attacks by using secure telecommunication protocols such as SPINS.

Changing the Traffic Data:

Changing the model of telecommunication data can prevent from analytic attacks.

The ability of transition the loop:

Moving the sensor loop can be useful in protecting from the space of private limits. The possibility of being attacked of sensor loops becomes less by moving them [7].

5-3] Attack by Discovering the Code of loop:

Discovering the code of loop is one of the most important problems in wireless sensor networks that results in heading internal attacks. When loops are being attacked, they are coded by laptop level's attacker and are programmed again and destructive codes are added to the sensor loop. Destructive codes are delivered to the network by this loop and disrupt the telecommunications of network [8].

Destructive activities can be the access of confidential information, the delivery of false report to the sensor network, starting the attacks of tracing and so on [9].

1-5-3. Protection against the Discovery of Coding the Loop:

The best way of confronting with the discovery of coding the loop is using the code of experiment designs. In this method, one optimal plan accepts the responsibility the process of research about the memory of loops to be informed about the truth of the memory of loops [10].

Another way is comparison of current situation of loops with previous situation of loops, while a loop is taken captive and is coded. It is planned again and delivered to the network again [11].

6-3. Sink Hole Attack:

In this attack, sink hole has false tracing information by one destructive loop of delivered packages and convinces delivered packages that there is a shorter way to arrive the destination and it catches them in a net. Sink hole is a special loop [or Zero loop] which catches loops in a net.

1-6-3. Protection against Sink hole Attack:

This attack has an effect on the layer of network and if delivered packages are given credit and controlled accurately, it can be possible to prevent from this attack.

A subordinate path should be traced for packages due to protect the loops while being produced the sink hole; therefore, a way is found for preventing the packages from being lost in sink hole. The neighboring loops of sink hole can also change their parents so that the flow of delivery the packages do not cross from sink hole loop and sink hole loop cannot receive any packages.

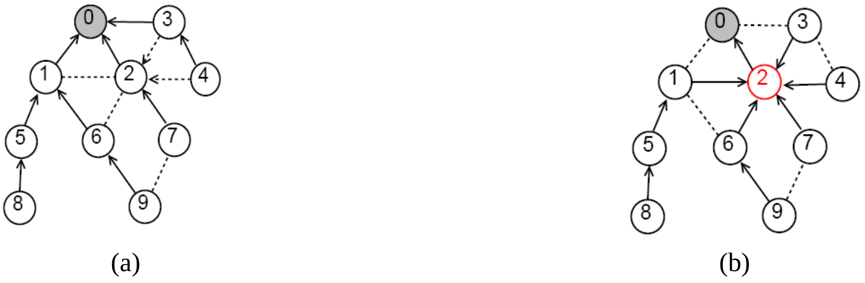

Fig. 1: a) Sensor network before being attacked by sink hole b] Sensor network after being attacked by sink hole [12].

7-3. Worm Hole Attack:

This attack occurs when a destructive loop delivers a tunnel of destructive loop to other points of sensor network. This attack disrupts tracing in the network and affects on the accumulation of data and sensor investigative protocols.

1-7-3. Protection against Worm hole Attack:

This attack affects on the layer of network and it can be prevented from emerging this attack by flexibility in tracing of network and controlling in it.

For example, the design of good tracing protocols such as multiple tracing can help these attacks to minimize. Another way is that each sensor loop has a common key with the main station that destructive loops are recognized by it.

8-3] Manipulation Attacks of Tracing Information:

A destructive loop can change the whole network by delivering false information to other loops in a network. These are the causes which produce this problem: running out of resources which are used by loops, producing loops while tracing, increasing the delay of delivery the information, an etc. This attack affects on the layer of network and it can be prevented by means of giving credit and coding the information.

9-3] Selective Forwarding Attack:

A destructive loop can select some packages of network and affects other packages of network by them and prevents from distribution of them in the network and controls the whole network.

1-9-3] Protection against Selective Forwarding Attack:

Multiple tracing can be used for protecting against selective forwarding attack that if destructive packages are sent in one route, it is possible that packages are delivered from another route.

Another way is creating the algorithms of identifying the behavior of loops that can be possible to identify attack due to incorrect behavior.

3) Standard Protocols of Wireless Sensor Network:

Improving the standard of WSN networks create their needs to provide special protocols for communicating with each other. These secure protocols can affect on the level of physical layer and MAC such as [802.15.4 IEEE] and they can be implemented on the layer of the network level such as protocols [ZigBee] and or over three layers such as Bluetooth. The weak points of these protocols cause attack to the network [13].

1-4] IEEE 802.15.4 Protocols:

This standard protocol is created on behalf of IEEE for secure telecommunications in wireless sensor networks. This protocol has tree modes such as unsecure operational mode, Access Control List [ACL], and secure mode. No secure service is created in unsecure mode. In Access Control List [ACL] mode, one list of pieces which can communicates is kept. In Access Control List [ACL], each piece which communicates in the network should be in this list, of course, no secure work is done for hiding and coding the data. In secure mode, all the secure services are presented: the control of access, coding and being confidential of data, comprehensiveness and repairing consecutive data.

Coding algorithms of AES-128 are used for all the secure stages and the highest amount of security will be existed by adding messages integrity code [MIC].

1-1-4] Evaluation of IEEE 802.15.4 Protocol:

Secure series of 802.15.4 protocol implement on the radio chips. All its calculations are done in the hardware and it causes the reduction of consuming energy.

The problems of inflexibility exist in key models of this standard protocol that these limits can overcome the highest secure protocols. If secure features which have been designed in 802.15.4 standard implement accurately can be the best basis of constructing higher secure levels.

2-4] ZigBee Protocol:

This standard protocol has been improved by ZigBee union which is an international industrial consortium in the area of semiconductor protection and its technologies. ZigBee standard has been made on IEEE 802.15.14 standard specifically, but ZigBee implements on the layer of network and practical layer [14].

Implementing the security in a message in ZigBee is possible by adding supporting header to the header of ZigBee's network layer and Message Integrity Code [MIC] is added to it after loading the message.

ZigBee uses the concept of trust to manage the security in a network; i.e. the coordinator of network can trust a method, in case, it recognizes the request of connecting to the network, keeps and distributes its keys and can have secure punctuated communication between the coordinator of network and other things.

1-2-4] Evaluating ZigBee Protocol:

The weak points of this protocol are using the secure series which create many problems for the messages. The longitudinal increase of higher than 30 Bites to the messages causes delay in sending the messages and consuming more energy.

ZigBee also has problems in its fundamental layer. An attacker can prevent of delivering the packages, while acknowledge of sending a package to the loop of the receiver has been sent. Another problem is that attacks preventing from Denial of Service [DOS] can send a harmful envelope to prevent from sending packages to that address while coding and hiding the information. This work is for the defect of messages. The receiver loop cannot recognize and code harmful envelope and it causes to reduce the efficiency of loop. Such cases that cause to reduce the ability of sending in the network also exist in this protocol [15].

3-4] Standard Bluetooth Protocol:

Bluetooth is a radio wave on the basis of telecommunication technology in short frequency ranges for wireless sensor networks [17].

Its mechanism is in such a manner when it discovers a thing, it informs all the things which are in the range of Bluetooth things to be able to communicate with it. Bluetooth has three secure modes: unsecure mode allows each thing to communicate with other available things. Second mode is the security of service levels that in this mode, secure procedures are created after creating telecommunication channels for controlling the accessibility of services and things. In third secure mode, the level of link among things that its secure procedures are created before telecommunication channel [18].

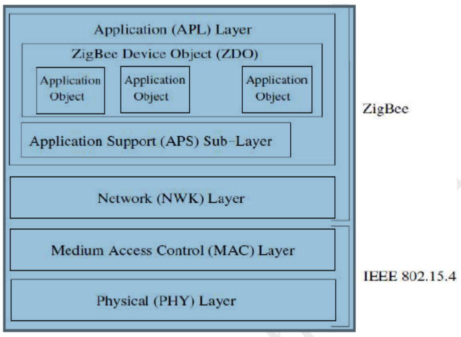

Fig. 2: the stack of ZigBee and IEEE protocols [16802.15.4].

1-3-4] Evaluating Standard Bluetooth Protocol:

Bluetooth protocol has weak points in implementing its stack that allows the stack to be attacked. In general, attacks in aggression to these protocols had been more successful than other telecommunication protocols and afflicted the security with problem easily [19].

Conclusion:

In this article, threats and attacks on wireless sensor network are recognized. Most important attacks of network were described elaborately such as: Denial of Service [DOS], Sybil attack, physical attack, attacks to the space of private limits, attack by discovering the code of loop, sink hole attack, worm hole attack, manipulation attacks of tracing information, and selective forwarding attack of packages. Ideas were described for protecting the wireless sensor networks. The most important standard protocols of wireless sensor networks; i.e. IEEE 802.15.4, ZigBee, and Bluetooth and their weak and strong points were described. IEEE 802.15.4 protocol can be the best basis to construct more developed secure protocols with consideration to the comparison of these protocols and the study of them and construct protocols with higher security in future. Also, I should find newer secure strategies in future work which can guarantee the security of wireless sensor networks more against attacks.

REFERENCES

[1] Law, Y.W., J. Doumen and P. Hartel, 2004. "Benchmarking Block Ciphers for Wireless Sensor Networks," in IEEE International Conference on Mobile Ad-hoc and Sensor Systems [MASS'04], Fort Lauderdale, Florida, USA, 447-456.

[2] Anderson, R. and M. Kuhn, 1996. "Tamper Resistance - a Cautionary Note," in The Second USENIX Workshop on Electronic Commerce, Oakland, California, USA, 1-11.

[3] Lee, J.C., *et al*., 2007. "Key Management Issues in Wireless Sensor Networks: Current Proposals and Future Developments", IEEE Wireless Communications, 14(5): 76-84.

[4] Lu, K., *et al*., 2008. "A Framework for a Distributed Key Management Schemein Heterogeneous Wireless Sensor Networks", IEEE Transactions on Wireless Communications, 7(2): 639-647.

[5] Newsome, J., E. Shi, D. Song, A. Perrig, 2004. ‘the Sybil Attack in Sensor Networks: Analysis and Defenses’. Proceedings of the Third international Symposium on Information Processing in Sensor Networks, 26-27.

[6] Deng, J., R. Han, S. Mishra, 2004. ‘Intrusion Toleranceand Anti-Traffic Analysis Strategies for Wireless Sensor Networks’, the International Conference on Dependable Systems and Networks.

[7] Chan, H. and A. Perrig, 2003. “Security and privacy in sensor networks,” Com- puter, 36(10): 103-105.

[8] Shi, E. and A. Perrig, 2004. “Designing secure sensor networks,” IEEE Wireless Commun , 11(6): 38-43.

[9] Seshadri, A., A. Perrig, L. Doorn and P. Khosla, 2004. “SWATT: Software-based attestation for embedded devices,” in Proc. IEEE Symp. Security Privacy, 272-282.

[10] Song, H., L. Xie, S. Zhu and G. Cao, 2007. “Sensor node compromise detection: The location perspective,” Proc. Int. Conf. Wireless Commun Mobile Comput, 242–247.

[11] Bryan Parno, Adrian Perrig, Virgil Gligor, 2005. "Distributed Detection of Node Replication Attacks in Sensor Networks," sp, 49-63. IEEE Symposium on Security and Privacy [S&P'05].

[12] Krontiris, I., Thanassis Giannetsos, TassosDimitriou, 2007. “Intrusion detection of sinkhole attacks in

wireless sensor networks” in Proceedings of the 3rd International Workshop on Algorithmic Aspects of Wireless Sensor Networks [AlgoSensors 07], Wroclaw, Poland.

[13] Tiny OS web site, http://www.tinyos.net/ [Last Visit: January 31st, 2005.

[14] Zigbee Alliance Web Site, http://www.zigbee.org.[Last Visit: January 31st, 2006]

[15] Rui Silva, Serafim Nunes “SecurityIssuesonZigBee” [2005],http://rtcm.inescn.pt/fileadmin/rtcm/WorkShop_22_Jul_05/s2_Security_Issues_on_ZigBee.pdf. Accessed: 5 January 2009.

[16] www.Prozhe.com/hesgar-bisim-zare-ab-zamin-[www.prozhe.com].pdf

[17] Charles Sturman, *et al*., “Bluetooth: Connect WithoutCables”, Prentice Hall PTR. ISBN: 0130898406.

[18] Bluetooth Special Interest Group, 2008. http://www.bluetooth.comaccessed.

[19] Karygiannis, T. and L. Owens, 2002. "Wireless Network Security: 802.11, Bluetooth, and Handheld Devices," National Institute of Standards and Technology NIST_SP_800-48.