J. Basic. Appl. Sci. Res., 2(2)1926-1932, 2012
© 2012, TextRoad Publication
ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Security and Common Attacks against Network Layer In Wireless Sensor Networks

Jalil Jabari Lotf, Seyed Hossein HosseiniNazhad ghazani

Department of Computer Engineering, Ahar Branch, Islamic Azad University, Ahar, Iran.

ABSTRACT

There have been a lot of researches carried out for improving security in wireless sensor networks recently. The reason for these challenges is the existence of sensor devices in military, observance and ecology control. But regarding the inherent limitations and the nature of sensors in this network, considering its energy resources and computational capabilities, security in sensor networks has been one of the challenging issues and they have critical differences compared with the security issues in traditional networks. Frequent attacks try to misuse unreliable communicative channels and work in unpreserved environments and penetrate into or destroy the network. In this article we will study security requirements and then represent the security obstacles related to sensor networks' grid layer.

KEY WORDS: Wireless sensor networks; attacks; security.

I. INTRODUCTION

The principle capability of wireless sensor networks is that they can be spread broadly in an environment and collect data from it and the place of sensor nodes is not necessarily predetermined or identified. This characteristic supplies us the ability to release them in dangerous or unavailable positions. Wireless sensor nodes use wireless communication method to connect with each other and each node has a limited radio range in which it can send the data. Thus, those nodes located in farther places from base should send their data to neighboring nodes in order to deliver the data to base after some steps. This threatens the security of data. Also sending the data using wireless connection can harm the security of data.

Regarding the things mentioned, supplying security in wireless sensor networks is a must and since nodes have limitations of energy, using high end encoding algorithms with less processes and low energy consumption requires a lot of care to avoid network's life span reduction benefitting from security supply in wireless sensor networks. On the other hand, we can mention security requirements in wireless sensor networks as follows:

- **Confidentiality of data**

Confidentiality means hidden maintenance of data from unauthorized parts. A sensor network should not allow the collected data by sensors penetrate into the neighboring networks. In most applications such as key distribution, the nodes communicate sensitive data and by maintaining confidentiality the data won't be delivered to unauthorized people. Data confidentiality in sensor networks should achieve the following goals:

1. Data achieved by sensor networks should not leak out the network.
2. Very important data such as coding keys should be secure in connections.
3. The general information about sensors such as identity and common keys should be encoded against traffic analysis attacks.

Encoding data with a secret key is generally accepted for preserving confidential data. In this case only the authorized receiver has the key code. Thus, this code is reliable.

- **Identification and Authentication**

In a sensor network, the enemy nodes can easily inject messages or destroy the packages' flow by adding extra packages. Thus, the receiver nodes should be assured of the validity of the sender which has started the sending process. In fact identification helps the receiver to be assured of the sender and authentication avoids sharing with unauthorized nodes in the network. Valid nodes should be able to discover messages received from unauthorized nodes and reject them. When two nodes connect, identification can be achieved by using a completely symmetrical mechanism. In this case, sender and receiver share a common key to measure Message Authentication Code (MAC). In other words, the sender and receiver have a common key to calculate MAC of the message which is used for all kinds of data connections between them. When a message with a correct message MAC is received, the receiver identifies that it has been sent from a valid sender and can easily identify the unauthorized sender and unauthorized message.

***Corresponding Author:** Jalil Jabari Lotf, Department of Computer Engineering, Ahar Branch, Islamic Azad University, Ahar, Iran.
E-mail: J-Jabbari@iau-ahar.ac.ir

- **Integrity of data**

By making the data confidential, external agents cannot steal it. But this does not mean we have secure and assured data. An external agent can change the data and make a chaos in the whole network. Integrity of data assures that the receiver receives appropriate data. Because other natural agents such as noise, weakening … can change the data, in addition to the attackers. In this case, we can be assured by preserving integrity of the correctness of the data received.

- **Freshness of data**

Data freshness can assure that the data received is new and does not repeat the previous ones. To solve this problem, we can use different types of time dependant counters which are added to data packages in order to show the freshness and newness of the data. SNEP security protocol uses this method to guarantee the freshness of data.

There are two types of freshness as follows:

1. Weak freshness: it provides a trivial order for messages, but does not transfer the data delay.
2. Strong freshness: it provides a general order for both demand and response of the messages and provides us to estimate the delays of messages before they arrive.

- **Robustness and survivability against the enemy**

A sensor network should be able to resist different attacks and threats against the network and if there is a successful attack, it should have the least undesired effect. When a network node is occupied by the attackers, security in the whole network should not be threatened.

I. Attacks in grid layer and related resistance

Generally the attacks in a wireless sensor network can be done in 5 layers. One of the layers in wireless sensor networks which face most attacks is grid layer. Routing is one of the basic duties of this layer. The common destroying attacks in this layer is selected forwarding, sinkhole attack, Sybil attack, Hello Flood attack, Misdirected attack, and Wormhole attack. In the rest of this paper we will focus on details of each one of these attacks.

A. Selective forwarding

Selective forwarding is one of the attacks which happen in wireless sensor networks. As it is implied by the name, in this attack the enemy node tries to direct all forwarded packages towards a certain node in order to remove a package from among received messages, randomly or the package's importance. In wireless sensor networks, usually all nodes take part in routing. Especially in multi-step method, each node participates in packages' routing to choose an appropriate sending route. Also selected forwarding attack uses the above-mentioned approach to reject the service (D. Ganesan, 2001).

The enemy node can choose removable packages regarding the data present in the message. For example, in military applications it removes packages which contain important information in military areas. In this case it should have a complete knowledge about the content of messages. Also it can achieve package selection based on used routing algorithms. That is, it can remove the messages used in routing algorithms and avoid forwarding to interfere the trends in routing process. The effect of this attack can be caused on factors such as enemy's position and message importance. The closer the enemy node to the sink, the more effective attacks will be there in these points. Also the importance of the messages which are thrown away show the effect amount of this attack. That is, the more importance over the overthrown messages, there would be more effective attacks.

Another kind of selected forwarding attack is black hole in which each message moving around this node will be destroyed. When a node sends a message without destroying it, it works as a repeater. That is whenever the package moves over this node, it does not increase the steps of the package and thus the receiver thinks that the package moves in fewer steps in a repeater node route. So it tries to use this package route in next sending in which selected forwarding uses to absorb packages towards it (Hang Liu, 1997).

- **Defense against selected forwarding attack:**
  - **a. Using observer nodes**

Some observer nodes are implemented in the network, which assure that the neighboring nodes send the received messages (Steven Cheung, 1997).

  - **b. Using watchdog**

Watchdog technique is in fact a kind of supervising and observance over the network. For example, supervising whether a node has sent a received message or not?

  - **c. Listening to a channel**

Another resolution is to listen to a channel to make sure that each node sends the same message which its neighboring node has sent.

d. Multi-step routing

Multi-step routing with random route selection is one of defense methods against selected forwarding attack. If the package moves in several routes towards the destination, there would be less probability to confront enemy node in all routes.

e. Sequential one to one search

In this defense method, the whole network is studied. It is determined if a message is not received, the reason is the traffic or an enemy node avoiding the delivery of it. In this case data sending route is changed and the enemy node or the affected node is identified (G. G. Finn, 1998).

f. Using encoding the data

As it is said earlier, basically this attack is done when the content of the packages is known by the attacking node to remove the important packages. Thus, if the content of the package is encoded by the code keys of each node, the enemy would not remove the package because it is not aware of the contents (Sergio, Marti).

B. Black hole attack

One of the common attacks in grid layer is black hole attack in which the attacking node tries to direct all packages of the network towards itself. In other words it tries to pull all the traffic towards itself. And in fact it tries to introduce itself as the sink. To do this, the attacking node introduces itself the closest node to the sink or considers itself as a node with extraordinary capabilities. It does this to encourage the neighboring nodes to choose the enemy node for routing their data (D. Ganesan, 2001).

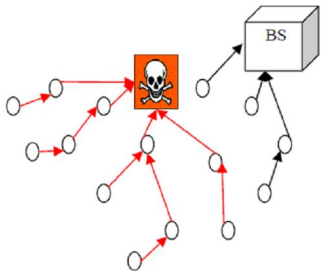


Figure 1: Black hole attack

If the enemy node does not introduce itself as the sink, the closer to the sink, it can make more interruptions in the network because the traffic absorbed by enemy node will be more. Figure 1 shows the performance and traffic absorption of enemy node. The attacking node can introduce itself as the closest node to the sink or it has the least steps towards the sink. If it can send message to all the nodes it has a state of worm hole attack. Also this attack can accompany selected forwarding.

In most routing algorithms, each node has a sending quality by which the quality of the generating node is shown. When it reaches below 25, updating is done. When up-dating, the nodes send their identity and the number of steps to the sink to the neighboring nodes. While a quality amount of each node is sent to the neighboring node, it introduces itself with its high quality black hole and fewer steps. In fact, this attacking node which serves as black hole uses the messages coming from the nodes to choose a node other than the black hole to make fake messages and convince the nodes generated that the route quality of the generating node is less than that of black hole (Jessica Staddon, 2003).

For example, consider that according to figure 2, there is a node like A1 which selects A2 as the generating node for itself. The attacking node notices that the route quality for itself is less than that of A2 node. Thus, it produces a fake message on behalf of A2 which decreases its route quality to below 25.

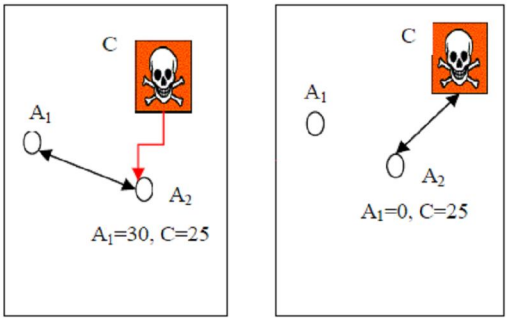


Figure 2: Creating incorrect communications by attacking node

When A1 node receives this fake message it up-dates itself in the table with the new value. When A1 tries to select a new generator for itself, it rejects A2 and chooses black hole. But if a new update is received from A2 node during fake message sending and new generator selection, the attack will not be practiced because sending quality is adjusted with the real amount.

- **Defense against black hole attack**
  - **a. Geographic forwarding**

Nodes are aware of their own and neighboring nodes' coordinates. Thus, each node can send messages according to the geographical position of the neighbors. So it is not absorbed easily towards the attacking node. In this method, nodes can send data from different routes regarding the coordinates of themselves or the neighboring nodes and avoid sending from a repeated and fixed route.

b. Using resistive routing protocols

Protocols resistant against different formations can also reduce the effect of this attack. These protocols do not confine themselves to the nodes' position in choosing a node as the next node to send data towards the sink and the nodes' remaining energy is efficient in algorithm selection. As soon as the network identifies a defect or detects incorrect data forwarding, it uses a systematic rerouting to avoid attacks. Those protocols which use serial number, when forwarding a package, can identify fake messages. Thus they are able to identify the messages sent by black hole node.

C. Sybil attack

This attack aims at destroying the limited memory of sensor nodes. In this case, the carrying node introduces itself with several identities and these identities are stored in sensor nodes' memory, while these nodes with the identities mentioned do not exist in reality and only are used to fill the memory of the sensor node. Figure 3 shows the performance of this attack.

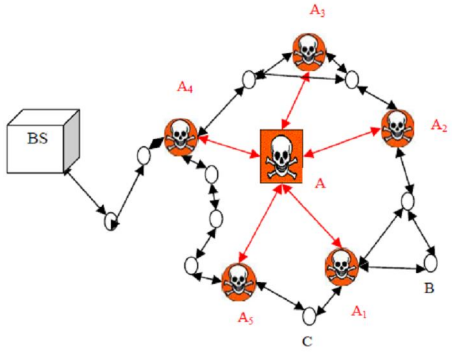


Figure 3: a design of Sybil attack

In figure 3, the enemy node with identity A introduces itself with the following identities (A1, A2, A3, A4, and A5) and different coordinates. When a node like B wants to forward data to a node like C, it uses a virtual node and an interface called A. That is, the node B believes that forwarding the data through A1 is more optimal, while this node does not exist really. In this way, all data forwarded to that node will be destroyed.

Usually wireless sensor nodes have a table of neighborhood in order to route and forward the data to the destination, in which there are some data such as each node's identity, the number of steps which should be covered in order to reach the destination, energy amount of each one of the routes in some protocols … which are stored. Thus, when this attack happens the memory of network's nodes is filled with unreal nodes. Since the memory is limited in these nodes, this virtual data clears the data related to the real neighboring nodes' data. But because at routing time these virtual and invalid nodes are utilized, nodes do not identify the incorrect forwarding in the network.

This attack not only inhibits the correct storage of the data and forward different data from different identities, causes some problems in synchronization, nodes' remaining energy and forwarding incorrect data and fair appropriation of the resources. Also it does not let the attack to be revealed or it denies the existence of the attack. In fact this kind of attack is a great threat for routing based on geographical position of nodes because in this type of routing algorithms, routing is done through the use of neighboring nodes' geographical position.

- **Defense against Sybil attack**

Nodes' validation is one of the defensive methods against this attack. In this case, authentication and reliability of the node should be investigated before accepting it as a neighboring node. For validation, usually code identification of messages is used (D. Ganesan).

In this method, the sink uses a valid key to validate nodes. Sometimes a periodical common key between the nodes is used to encode the communications. An application sample of this validation is used in SPIN protocol (Naveen Sastry, 2003). Regarding the fact that in this attack the adversary node introduces itself with different identities and coordinates, a resolution to make sure of the position and coordinates of nodes is that we can verify the correctness of these coordinates through received signals (Siebe Datema, 2003).

D. Hello Flood attack

Hello Flood is another common attack against wireless sensor networks. In most routing protocols, nodes need to generally distribute Hello packages to announce their existence to other nodes. In fact this message is used to discover the route and make changes and create neighborhood tables. The node which receives this package imagines that it is located in the radio range of the forwarding node. However, this imagination can be wrong. An interfering agent of laptop, generally distributes routing data or other data with a great forwarding capability and convinces each node in the network that it is the neighboring node. Thus, authorized nodes in the network will try to forward their data to the attacking node, those which are out of the boundary, because those nodes will not receive these messages (Wassim Znaidi, 2008).

- **Defense against Hello Flood**

By studying the bilateral local communications before starting to connect, it would be a suitable approach for attacker to have the same capabilities as sensors have. That is it is located at the same working frequency as the sensor node or it can estimate its distance from that node by knowing its distance and get assured of the authenticity of the forwarding node. However, if the carrier uses a sensitive receiver it can convince the nodes about the lawfulness of itself (D. Ganesan, 2001).

Also the existing validation system is an effective defense method against Sybil attack. It uses three validating nodes to approve the neighboring nodes before messages are forwarded.

E. Incorrect route attack

The attacking node misdirects the nodes by forwarding messages from wrong and incorrect routes. When nodes update the forwarded routes in their routing tables, this node usually misdirects through incorrect announcement of the routes. Through this attack we can focus the traffic around a node to destroy the node because of forwarding and receiving messages and overusing the energy. Also this attacking node is able to cause traffic in the network by forwarding fake messages and corrupting the messages forwarded. It selects the victims from among nodes close to the sink and by stopping these nodes other connections with sink will also be stopped (Anthony D. Wood, 2008).

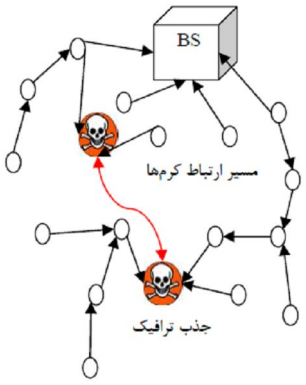
- **Defense against incorrect route attack**

An effective method against this attack is to reevaluate the routing tables of the nodes when updating to avoid changing them by enemy nodes. Also the novelty mechanisms of the data can avoid the repeat of the data by investigating them. In this way, repeated messages are thrown away and this will preserve the network from repeated messages and node's memory filled.

In wireless sensor networks which use hierarchical structure for routing, there are filters which test each message before forwarding. Messages with source addresses which are lawfully located in lower levels of hierarchy will be overthrown.

F. Worm hole attack

In worm attacks, the enemy nodes have connections with each other in a different frequency which is different from that of the network's connection nodes. In this case network nodes will not be able to detect these connections.



For example, two attackers may have radio forwarding in frequencies with long wave or distant wireless connection to communicate with each other. Also they are considered to have great capabilities and are able to convince the authorized nodes in the network. In this way the data will move in a shorter step and absorbs the traffic in the network towards itself. Usually one of these nodes is located near the sink and the other node which is farther forwards the received data to another worm node. Since the attacker creates a new qualified route to the sink by bonding with worm hole, all traffic in it is caused by this current bond and thus a black hole attack is created (Y. C. Hu, 2003).

Because it is possible that all traffic in the network is directed towards worm nodes, the network will be left in an inconsistent state in which some services should be reinstalled to store a suitable performance.

- This attack also can be done by utilizing a single enemy node in which the attacking node distributes the packages between the two authorized nodes in order to convince the neighboring nodes.
- The attacks by worm hole can accompany selected forwarding or overhearing. Identifying this attack in integration with Sybil attack is very difficult.

- **Defense against worm hole**

As it is described about black hole, geographical forwarding will be achieved through a routing protocol with resistant negotiations. Each message is forwarded singly. Selection of the next node is done by informing about the geographical position of the node. Such a design will not create a hole in the network, although sometimes it can be achieved randomly.

HU & et al described a defense method based on triplex packages in which the distances of a message may be covered in a single step. Each message includes time period and forwarder's position. The receiver compares them with its position and the time to determine whether the highest transformation range has been observed or not. This resolution requires careful timing and approving the exact point. It is possible to limit the application to wireless sensor networks (Y. C. Hu, 2003).

II. Conclusion

As it is said, several attacks are done in grid layer of the wireless sensor networks which can halt the correct performance of the network. Also the enemy node can collect the data from the environment and use the data to benefit for itself. Different methods for prevention or defense against these attacks have been proposed which can reduce their effect as much as possible. In protocol and varied algorithms designing of sensor networks, preserving the security and defense against the attacks is one of the principle and critical issues for investigation.

For this reason the data forwarded between nodes are encoded to need decoding when overheard by the enemy and not to access the main data without having the key. But encoding needs a lot of energy consumption and memory regarding the greatness and the number of operations. Thus, there should be a balance between security supply and the amount of using limited resources in sensor nodes.

REFERENCES

Ganesan, D., Govindan, R., Shenker, S. & Estrin, D. (2001). **Highly-resilient energy-efficient multipath routing in wireless sensor networks** IEEE network.

Liu, H., Ma, H., Zarki, M. & Gupta, S. (1997). **Error control schemes for networks: An overview. Mobile Networks and Applications**. 2(2):167-182.

Cheung, S. & Levitt, K. (1997). **Protecting routing infrastructures from denial of service using cooperative intrusion detection**", In New Security Paradigms Workshop, Cumbria, UK.

Finn, G. (1987). **Routing and addressing problems in large metropolitan-scale internetworks**, TechnicalReport ISI/RR-87-180, ISI.

Venugopalan, P., chagari, P., Dean, A., Mueller, F., Sichitiu, M.(2003). **Analyzing and Modeling Encryption Overhead for Sensor Network Nodes.** 2003 ACM 1-58113-764.

Znaidi, W., Minier, M. & Philippe, J. (2008). **An ontology for Attacks in Wireless Sensor Networks.**

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE, October 2008, 13 pages.

Xu, W., Ma, K., Trappe, W. & Zhang, Y. (2006). **Jamming sensor networks: attack and defense strategies.**Network, IEEE, 20(3):pages:41-47.

Law, Y., Hoesel, L., Doumen, J., Hartel, P. & Havinga, P. (2005). **Energy-efficient link-layer jamming attacks against wireless sensor network mac protocols.** In SASN '05: Proceedings of the 3rd ACM workshop onSecurity of ad hoc and sensor networks, pages 76-88, New York, NY, USA.

Wood, D. & Stankovic, A. (2002). **Denial of service in sensor networks.** IEEE Computer, 35(10):54.62.

Hill, J., Szewczyk, R., Woo, A. Hollar, S., Culler, D. & Pister, K. (2000). **System architecture directions for networked sensors.** In Proceedings of ACM ASPLOS IX.

Aleksejev, Jevgeni, Jutman, Artur, Ubar & Raimund (2006). **LFSR polynomial and seed selection using genetic.** IEEE Symposium on System application.

Zhu, S., Setia, S. & Jajodia, S. (2003). **LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks.** 10th ACM Conference on Computer and Communications Security (CCS'03), Washington D.C.

Karlof, C., Sastry, N. & Wagner, D. (2004). **TinySec: Link Layer Security Architecture for Wireless Sensor Networks.** *ACM SenSys 2004*.

Hu, Y.-C., Perrig, A. & Johnson , D.B. (2003). **Packet leashes: a defense against wormhole attacks in wireless networks.** In Proc. IEEE Infocom 2003, 3, 1976–1986.

RAMARAJ, A. (2006). **MODELING OF SENSOR NETWORKS – ATTACK SURFACE, QOS SURFACE.** Submitted to the Faculty of the Graduate College of the Oklahoma State University in partial fulfillment of the requirements for the Degree of MASTER OF SCIENCE.