International Journal of Informatics and Communication Technology (IJ-ICT)
Vol.8, No.1, April 2019, pp. 13~18
ISSN: 2252-8776, DOI: 10.11591/ijict.v8i1.pp13-18

Security in wireless sensor networks

Bahae Abidi[1], Abdelillah Jilbab[2], Mohamed El Haziti[3]
[1]LRIT Associated Unit with CNRST (URAC 29) Faculty of sciences, Mohammed V University in Rabat, Morocco
[2]ENSET, Mohammed V University in Rabat, Morocco
[3]Higher School of Technology, Sale, Morocco

Article Info

Article history:

Received Oct 1, 2018
Revised Dec 10, 2018
Accepted Jan 4, 2019

Keywords:

Aggregation
Authentication
Flexibility
Security
Wireless sensor networks

ABSTRACT

Even in difficult places to reach, the new networking technique allows the easy deployment of sensor networks although these wireless sensor networks confront a lot of constraints. The major constraint is related to the quality of information sent by the network. The wireless sensor networks use different methods to achieve data to the base station. Data aggregation is an important one, used by these wireless sensor networks. But this aggregated data can be subject to several types of attacks and provides security is necessary to resist against malicious attacks, secure communication between severely resource constrained sensor nodes while maintaining the flexibility of the topology changes. Recently, several secure data aggregation schemes have been proposed for wireless sensor networks, it provides better security compared with traditional aggregation. In this paper, we try to focus on giving a brief statement of the various approaches used for the purpose of secure data aggregation in wireless sensor networks.

Corresponding Author:

Bahae Abidi,
LRIT Associated Unit with CNRST (URAC 29) Faculty of sciences,
Mohammed V University in Rabat, Morocco.
Email: bahae.abidi@gmail.com

1. INTRODUCTION

A wireless sensor network (WSN) [1] is a wireless network, built from a few to several hundred or even thousands of nodes, where each node is connected to one or several sensors which communicate through a wireless link, as it shows in Figure 1. It consists of sensor nodes that capturing information from an environment, processing data and transmitting them to the base station or destination. These nodes are characterized by a low size, a low complexity device with low cost, which communicates through a wireless link. In addition, wireless sensor networks confront same difficulties, such as limited power supplies, low bandwidth, small memory sizes and limited energy.

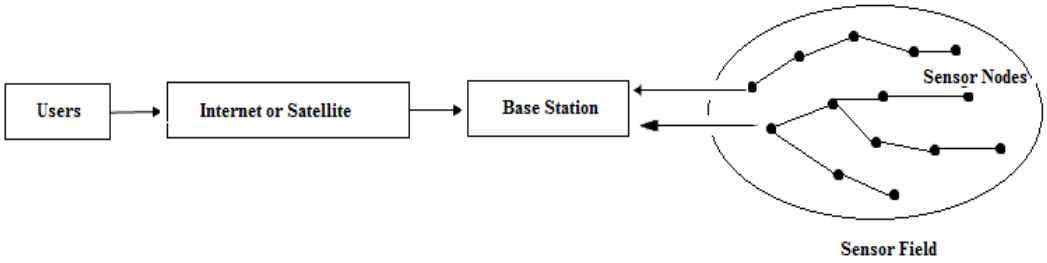


Figure 1. Structure of Wireless Sensor Network

In order to respond to these various constraints, multiple routing protocols were implemented. These routing protocols have been developed to help nodes to exchange their information, data are routed to reaches the sink, finding an optimal routing tree to connect sources to sinks, depending on the network organization, different ways are used according to the routing strategy. There are several methods, techniques, and algorithms used to fuse data: like clustering, fusion, aggregation. Who have to increase the network lifetime, all that with maintaining efficiency and quality of information.

Clustering [2] is a self organization of the network nodes into clusters, according to some rules, to decrease the number of transmitted messages to the base station and thus reduce the size of the routing table stored at the individual node. Members of a cluster can communicate with their cluster-head (CH) directly and the CHs can forward data to the base station.

To describe the aspect of the fusion, several different terms have been used like data fusion, information fusion. The information fusion can be defined as the combination of multiple sources to obtain improved information with cheaper cost and greater quality. Concerning the term of data aggregation [3], it becomes popular in wireless sensor networks as a synonym for information fusion. Aggregation is the ability to summarize, which means that the amount of data is reduced, and the volume of data being manipulated is reduced also.

Providing a robust data aggregation protocol is a challenge because these aggregated data can be the subject of several types of attacks. So provides security is required to resist against malicious attacks, while maintaining a secure communication between various nodes in the network, facing the different constraints and adapting to the topology changes. Several secure schemes of data aggregation for wireless sensor networks have been proposed and it provides better security compared with traditional aggregation.

The paper is organized as follows: Section two deals with the use of security mechanism in the network, in section three we define some different attacks in wireless sensor networks, section four with giving a brief statement of the various approaches used for secure data aggregation in wireless sensor networks and finally we conclude in section five.

2. SECURITY IN WSN

To design a low power wireless sensor networks, energy optimization is a critical issue, without forgetting the use of a secure mechanism to protect our network. The energy consumption may not be negligible compared to the actual transmit power, to perform the sensing phases, the research will be aimed at the development of efficient systems able to directly use the antenna. The antenna plays a significant role in the overall reliability of the network, since it must guarantee the communication despite the difficult environment in which it has to operate [4-6], also the choice of the antennas to be exploited for the wireless sensor network realization can save our network from the different attacks, because the security becomes critical in wireless sensor networks in view of a large number of nodes. The security requirement for wireless sensor networks are similar to the others networks, a multi-hop communication is preferred, and the data can be sent by any node depending on the topology of the network.

2.1. Authentication

The authentication is a measure of security [7], each member of the network is authenticated before revealing information, it's a fundamental mechanism for access control in the network. Generally, the authentication is the process of verifying the identity of someone or something. If the authentication failed, an attacker can join the network and inject the wrong data. We have three types of cryptographic functions used for authentication: the hash function, secret key function, and public key function. But the traditional authentication based on public key cryptography is not suitable for wireless sensor networks, due to limited bandwidth and communication being most expensive in terms of energy. The message should not be extended significantly in length when we apply the security service. For that, in wireless sensor networks, we use two types of authentication: the device level authentication means a message is proved to originate from a specific device, and the group level authentication message is proved from a group of devices.

2.2. Confidentiality

The confidentiality is the property that information is not made available to unauthorized processes [8]. It provides privacy in the network, all information should be kept secret, that's mean, we have to encrypt the data with a secret key.

2.3. Freshness

The freshness is an important measure required by the sensor because this service makes certain that the transferred data on the network are recent. How is that done? It's simple, the major concept is to maintain

a table which contains the last value received from every sender, that's mean, we have to include an increasing counter with every message and reject message with old values.

2.4. Availability

For this concept, in wireless sensor networks, it means, that our network must face the various constraints related to the topology with the limited resources, and be available to provide services and authorize the communication.

2.5. Integrity

For example, a malicious node may add some manipulated data within a packet. This new packet can then be sent to the original receiver. So the integrity, ensuring that the message being transferred is never modified by any adversary without being detected.

3. ATTACKS IN WIRELESS SENSOR NETWORKS

Sensor networks are particularly suitable to several types of attacks, each one with her own goals. In this section, we will present some famous attacks in wireless sensor networks.

3.1. Sybil attack

Are major routing attacks and a harmful threat to sensor networks, a malicious node try to have more advantage than the legitime nodes [9], [10]. An adversary can be in more than one place at once, how that? A malicious node can claim different identities to other nodes in the network which can significantly reduce the effectiveness of fault tolerant schemes such as distributed storage, dispersity, multipath. Newsome and al. propose to classify the Sybil attacks in three dimensions:

The first one consist of direct communication to indirect communication:

- Direct: the malicious nodes communicate directly with the legitime one.
- Indirect: the malicious nodes communicate through other malicious nodes proclaiming able to achieve them.

The second one consist of fabricated identity, stolen identity:

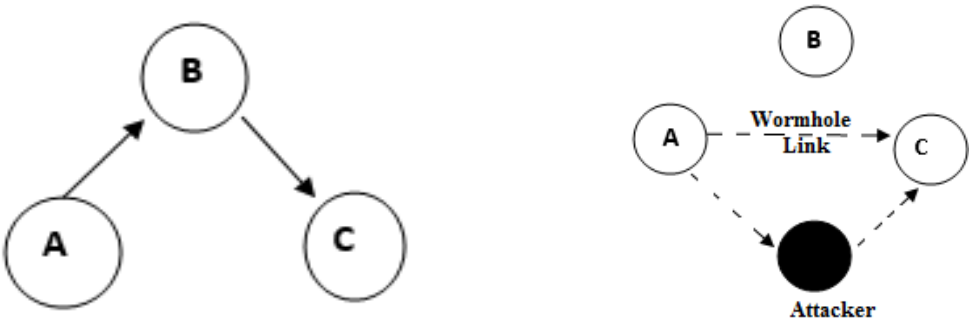
- A Sybil node can create an identity.
- A Sybil node can stol the identity of legitime nodes.

The third one consist of simultaneity:

- The attackers can involve all its identity in the network in a simultaneous way.
- The attacker can present just a parts of its identity over a given time period.

3.2. Wormhole attacks

The wormhole attacks can destabilize or disable wireless sensor networks. The attacker receives the packets at one point in the network, forwards them through a wireless link with much less latency than the network links, and relays them to another point in the network. Figure 2 shows an example of a wormhole attack.



(a) (b)

Figure 2: Wormhole attack

3.3. Denial of Service attacks

The denial of service attack can reduce the wireless sensor networks availability [11]. It is any occurrence that diminishes or eliminates a network's capacity, it's a simple event that prevents the normal functioning of its services. Denial of service is to prevent the normal operation of sensor victim by sending a lot of unimportant messages and denying access to other users.

3.4. Physical attacks

The wireless sensor networks are deployed in hostile environments, they are susceptible to many types of physical attacks due to the unsafe and unprotected communication network. The physical attack is an unattended operation, one of the most malicious attacks and harmful attacks on wireless sensor networks. All physical attacks have the ability to deal extra damage, an attacker will aim to recover the key used for encryption. An attacker can also reprogram the sensor to disrupt the network and the application voluntarily causing the abnormal behavior of the node.

3.5. Data corruption attacks

Data corruption attack is a type of attack on transit. Data corruption is caused by an attack on data in the network layer. These types of attacks are among others to create loops or draw him away from the traffic, generate false errors. How this? The attacker can repeat, delay or modify the content of messages during the transit.

4. DATA AGGREGATION SECURITY

4.1. Literature Schemes

Ozdemir [12] proposed Secure Reliable Data Aggregation. The authors indicate that the only cryptography cannot guarantee sufficient security for wireless sensor networks and propose a trusted network. The major idea is that each sensor node observes the behavior of its neighbors to develop a trust level. For this, monitoring mechanisms are used to detect the availability of the node and the bad behavior of neighbors. Secure Reliable Data Aggregation can detect if an aggregator is the subject of a denial of service attack. The authors claim that this approach involves a charge of tolerable communication while significantly increasing safety in the aggregation process.

Przydatek and al.[13] proposed a secure data aggregation, this is one of the first solution proposed by the scientific community. This solution is designed to calculate with the secure manner the aggregation function. So with that, the user can not only accept data with high probability if the aggregate result is a good approximation of the actual result, also the user can detect the attack with high probability and reject the result if it is outside of the limit. The authors proposed the approach 'Aggregate Commit Prove' in which the aggregator not only aggregates data but also proves that performs this task correctly. The first step consists of collecting data from sensor node by the aggregator and then locally computes the corresponding aggregate data. Concerning the second step, the aggregator is committed to providing a proof ensuring that the aggregate is well given collected. The server will be verified this evidence. The freshness of data is ensured with the change of dynamic keys, after each defined time interval. And the authentication with data integrity, they are ensured by using the message authentication code.

To provide efficiency and confidentiality in wireless sensor networks, Castellucia and al [14] proposed an efficient aggregation of encrypted data as a solution. They propose an additive homomorphic encryption while providing security of aggregated data. The main idea is to replace the XOR operation by a simple modular addition. The proposed system is probabilistic and this feature makes the complicated cryptanalysis since the sensed measure is covered by the injected random value. However, the source of this value constitutes the greatest threat against the analysis of encrypted data. It is possible to predict the next random value, this would mean a total rupture of the system. The security is also ensured against a replay attack since a new key is associated with each new message.

Yang and al [15] proposed a security protocol for data aggregation, 'Secure hop by hop Data Aggregation Protocol'. How can the base station get a good approximation of the aggregate in the presence of some compromises nodes? This approach tries to answer this question. So the authors propose various solutions in the security of aggregation such as the construction of the key distribution. They are based on the idea that in a hierarchical approach, nodes located near the base station calculates an aggregate that concerns large numbers of sensors. The system consists of two phases to avoid making more confidence in this type of nodes. In the first phase, the system uses a probabilistic approach that divides the network into the same size groups and a leader is elected in each group. In the second phase, aggregation is performed in each group, and each group suspected part in a certification process to prove the validity of his aggregate. She starts by authenticating group leaders, then verifying that the received message authentication code is original from

the supposed leader. The base station interacts with the group suspected to prove the validity of his aggregate.

Boudia and al. [16] proposed encryption data aggregation, this approach had to ensure the essential security needs with various function. In this one, the base station starts the sensing process by sending a broadcast message to the sensor nodes which are located in the area of interest. Sensor nodes then report back with their reading to the base station through an aggregator. The aggregator then processes the received readings of sensors. The sensor must have the knowledge about aggregation function which is used for the aggregation of sensor's reading. Every sensor nodes have their distinct private key shared with the base station which is computed by taking hash on the master key of the base station with their respective identifiers. More to this, each sensor node shares a pair-wise key with their children which is used for encryption.

4.2. Limits of Literature Schemes

Each system according to there specific characteristics have some advantages and disadvantages. In this paragraph, we will try to discuss the limits of the different schemes that we have mentioned in the previous paragraph. Concerning the first approach of Ozdemir, it provides high data confidentiality and authentication, but it's vulnerable to attacks and this is due to the key size. The second approach of Przydatek and al. guarantees perfect resilience, because the information is not dispersed on the shared key between two non compromised nodes. But if a single node is compromised, the security of the whole network is compromised. The attacker can put many more nodes in a critical situation, in order to damage the communication links and the amount of memory is extremely limited. The approach of Castellucia and al. provides high security and this is due to the use of the elliptic curve cryptography but it has limited ability to protect private key, without forgetting that the integrity is not checked. In Yang and al. approach, The data to be encrypted is divided into several texts but it's inefficient because not robust operations are applied in encryption, which weakens the algorithm and the data security. The advantage of the approach of Boudia and al. ensured a detection of anomaly nodes but only the final aggregate is verified, so if the verification fails, an important number of encrypted packets will be lost.

4.3. Security Analysis

In this part of our work, we will compare the different schemes in terms of the security performances, which means the different attributes that we studied in section 2. There are some schemes which provide more than one service like the scheme of Boudia and al. with that of Ozdemir which ensure: Confidentiality, Integrity, Authentication, and Availability. Concerning the scheme of Yang and al., he provides Confidentiality, Integrity, and Authentication, but that of Castellucia and al. Confidentiality and Freshness. Finally the scheme of Przydatekand al. ensure both, Integrity and Authentication. We notice that each solution provides various security services to resist against an attacker; for example the schemes of Przydatek and al. , Yang and al. are more robust because they can resist to three different attacks from the attacks in section 3: Denial of Service, Sybil attack, and Physical attacks. Contrary to the scheme of Ozdemir can resist to just Sybil attack. But that of Boudia and al. with Castellucia and al. can provide security in front of Denial of Service and Sybil attack.

5. CONCLUSION

Security in wireless sensor networks is the more important things to ensure the routing of data from the source to the destination, the need for security in WSNs becomes more apparent. Especially in the recent years, it has attracted a lot of attention because it's very challenging to design strong security algorithms. In this paper, we have described some requirement of wireless sensor networks and security problems, we have also surveyed some proposed schemes for securing data aggregation. Finally, we have discussed the limitation and security analysis of these schemes.

REFERENCES

[1] Samayveer Singh, A K Chauhan, Sanjeev Raghav, Vikas Tyagi, Sherish Johri, *Heterogeneous protocols for increasing the lifetime of wireless sensor networks*, Journal of Global Research in Computer Science, vol.2, no.4, April(2011), 172-176.

[2] Wesam Almobaideen, Khaled Hushaidan, Azzam Sleit, Mohammad Qatawneh, A Cluster-Based Approach for Supporting Qos in Mobile AdHoc Networks, International Journal of Digital Content Technology and its Application, Vol. 5, No. 1, (2011), 1 - 9.

[3] Eduardo F.Nakamura, Alejandro C.Frery, ANTONIO A., Information Fusion for Wireless Sensor Networks: Methods, Models, and Classifications, ACM Computing Surveys, Vol. 39, No. 3, Article 9, August 2007.

[4] S.K. Jayaweera, "Virtual MIMO-based cooperative communication for energy-constrained wireless sensor networks," IEEE Transactions on Wireless Communications, vol. 5, n. 5, pp. 984-989, 2006;
[5] P. Rocca and A. F. Morabito, “Optimal synthesis of reconfigurable planar arrays with simplified architectures for monopulse radar applications,” IEEE Trans. Antennas Propag., vol. 63, n. 3, pp. 1048-1058, 2015.
[6] C. M. Kruesi, R. J. Vyas, and M. M. Tentzeris, "Design and Development of a Novel 3-D Cubic Antenna for Wireless Sensor Networks (WSNs) and RFID Applications," in: IEEE Transactions on Antennas and Propagation, vol. 57, n. 10, pp. 3293-3299, 2009.
[7] Shantala Patil, Dr Vijaya Kumar B P, Sonali Singha, Rashique Jamil, A Survey on Authentication Techniques for Wireless Sensor Networks, International Journal of Applied Engineering Research, Vol. 7, No.11, 2012.
[8] B.Veeramallu, S.Sahitya, Ch.Lavanya Susanna, Confidentiality in Wireless Sensor Networks, International Journal of Soft Computing and Engineering, Vol.2, Issue-6, January 2013.
[9] Newsome, J., Shi, E., Song, D, and Perrig, A, The Sybil Attack in Sensor Networks: Analysis and Defenses, Proc. of the third international symposium on Information processing in sensor networks, 2004, 259 - 268.
[10] Douceur, J.The Sybil Attack, 1st International Workshop on Peer-to-Peer Systems 2002.
[11] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, Security in Wireless Sensor Networks: Issues and Challenges, ICACT2006, Feb 2006, 20-22.
[12] S.Ozdemir, H.Ichakawa et al. Secure and Reliable Data Aggregation for Wireless Sensor Networks, (Eds.), LNCS 4836, 2007, 102 – 109.
[13] B.Przydatek, D.X.Song, A.Perrig, Secure Information Aggregation in Sensor Networks, Conference On Embedded Networked Sensor Systems, 2003, 255 - 265.
[14] C.Castelluccia, E.Mykletun, G.Tsudik, Efficient Aggregation of Encrypted Data in Wireless Sensor Networks, MobiQuitous, 2005, 109 - 117.
[15] Y.Yang, and al., A Secure Hop-By-Hop Data Aggregation Protocol for Sensor Networks, ACM Transactions on Information and System Security (TISSEC), 2008.
[16] M.Boudia, O.Rafik, M.Feham, Secure and Efficient Aggregation Scheme for Wireless Sensor Networks using Stateful Public Key Cryptography, 11th International Symposium on Programming and Systems (ISPS), 2013, 96 - 102.