Investigation authenticity verification protocols in wireless sensor networks and propose a suitable authenticity verification protocol

Ali Akbarian

MSc student of encryption, University of Imam Hossein
azaryali@ymail.com

Abstract: Thereof protocols in wireless sensor networks could not have any complex computation because of energy and memory constraints. So the light thereof protocols in networks with symmetric encryption algorithms must be used for construction of summary functions. Some authenticity verification protocol and objections in this regard have been investigated and then examined the expression them and finally an affordable and lightweight authenticity verification protocol offered not only good but also has the previous protocol, and deliver on them, this protocol is quite high.

[Ali Akbarian. **Investigation authenticity verification protocols in wireless sensor networks and propose a suitable authenticity verification protocol.** *N Y Sci J* 2014;7(4):53-57]. (ISSN: 1554-0200). http://www.sciencepub.net/newyork. 10

Keywords: authenticity verification protocols, wireless sensor networks, a symmetric encryption algorithm, abstracting functions, lightweight

1. Introduction

Wireless sensor networks, due to reduced production costs and streamlined, the speed of fans have become very large around the world. Limited energy resources, data storage and computational constraints in these networks make additional security techniques other than traditional networks to be implemented.

One of the most important securities thereof services that its main purpose is to ensure the authenticity and genuineness of a relationship. Methods and tools to implement these services are available. For example, one of the most common ways to use encryption tool that will help meet this goal, the protocols are designed thereof.

Given the importance of the protocols in computer networks depends on many services, network security protocols thereof, there are tools and tools for analysis and verification of security protocols seems necessary.

2- Study thereof protocol

In 1981, Lamport [1, 2] proposed a password-based protocol thereof has used the hash chains. Although his protocol has computational and memory constraints faced by wireless sensor networks is not suitable, but the chain of hash functions that are suitable for sensor network protocols are studied him for a start.

This protocol is based on a disposable key is hash chain. In this protocol, Alice randomly chooses w - slow. A hash function to generate a sequence of keys (w, H (w), H (H (w)), ..., Ht (w)) are used. That Ht (w) means that the function H, t is repeated. I th key thereof to Ht-i (w) wi = is defined. Lamport protocol is shown in Algorithm 1.2. The last member of the sequence of the function keys hash, t is repeated a call w_0. (Signs algorithms are listed at the end)

It is clear that this protocol is able to meet all the requirements of sensor networks, wireless is not, because sensor network Wireless - Wireless with limited power and memory are facing and protocols thereof lamport need more than 1 kbps diagnostic accuracy for each package. The implementation of this protocol is not suitable for sensor networks Furthermore, this protocol attacks are weak in terms of resistance to the use of hash chains thereof in sensor networks are very common.

Algorithm 1.2: Lamport Protocol
1. Initial phase, A value approach to verification w_0 for w_0 B sends entity B amounts to stores and counters j j = 1 is initialized. 2. For i = 1 to i = t thereof the following operations are performed. 3. A value of wi, and i will send to user B. 4. B term i = j and H (wi) = wi-1 does not check. If it was true, B will store the value of wi, and set j = j +1 will do for the next meeting.

Here we examine additional protocols concerning Gay Fawkes protocol thereof is [1,3].

The protocol in 1998, Mr. Needham, Anderson and his colleagues at Cambridge University presented) Algorithm 2.2 (. Within the structure of a protocol Hash functions are used to ensure authenticity of the message.

Algorithm 2.2 Guy Fox thereof Protocol

1. A random selection of K0 and H (K0) to user B sends.
2. Message Mi for i = 1 to i = n, so that the loop is repeated.
3. A new key Ki select a value ai = MAC (Mi ‖ H (Ki), Ki-1) can be calculated.
4. A statement released to ai.
5. A value of Ki-1, H (Ki) and Mi is sent to user B - slow.
6. B correctly, ie ai = MAC (Mi ‖ H (Ki), Ki-1) to test and then evaluate whether Ki-1 code word is implemented in the final round or not?

In the obligation to publish a key K0 H (K_0) is created. At any stage thereof, he promised a new key Ki H (Ki) creates and MAC on Mi and H (Ki) of Ki-1 key can be calculated. After the release of the MAC Alice Ki-1, all recipients can open the message Mi to verify. This protocol does not use a hash chain, but the chain ai uses. Each message includes a commitment to the key thereof used for the next stage thereof. This protocol requires that Alice knows Bob's public commitment to create ai ai has received. The disadvantages of this protocol is that the user B to user A wants to get to know the ai values for user A (Mi, H (Ki), Ki-1) to send to B, then B can authenticate A user can authenticate.

In continuation thereof TESLA protocol for wireless sensor networks can offer. The protocol presented in 2002 by Adrian Perrig the University of Berkeley. Another version of it in 2004 as part of the security protocol SPINS µTESLA has been [4]. This protocol is based on the protocol works best µTESLA thereof protocol for wireless sensor network is one of efficient protocols. In this protocol, the key distribution protocol for initial verification key K0 hash-chain is used [1, 5].

TESLA protocol thereof different approach by adding time offers. In this protocol, the sender (Alice) initially produces a sequence of hash keys temporarily as follows:

$K_n, K_{n-1} = H(K_n), \ldots , K_0 = H(K_1)$

The first end member (K0) over a secure channel for all users spread. Then, confirmed by Ki Mi Alice sends the interval ti. The messages are sent only in the interval ti.

Next time intervals Alice opens the key Ki and Mi users to confirm. The protocol is presented in Algorithm 3.2.

We note that users can receive messages before the receiver must be able to store them in memory.

In addition, this protocol requires synchronization between the transmitter and receiver. Otherwise, when a key opens an attacker can use it to forge messages.

To provide synchronization, we need a protocol to secure thereof. So basically an authentication protocol thereof for the time needed. In wireless sensor networks due to resource constraints and memory can not be used for asymmetric protocols hence, the tendency is symmetric protocols. Tesla protocol for wireless sensor networks cannot meet all needs. Because the primary key of the digital signature verification protocol for sensor networks that has very high computational load.

Decryption key is stored in each packet sent requires large power consumption is a key node in a large amount of disposable occupies.

The advantage of this protocol is that the computational cost to generate and verify the information provided below and can be a lot of information. This protocol uses a timestamp and it makes a lot of attacks can be prevented from occurring. Used in the hash function must be collision-resistant.

Algorithm 3.2 Tesla protocol thereof

1. Find A key K0 is the first sign and the expression S = SIG (K0, SK) releases. The S each recipient confirms. (S Signature private key (K_0) and SK is user A)
2. For message Mi in the interval ti i = 1 to i = n loop is accomplished.
3. A phrase Xi = MAC (Mi, Ki) calculated values of Xi Mi releases.
4. Each receiver will check whether Mi and Xi in the interval ti is received or not? And then store these values - slow.
5. A period t + 1 amounts to Ki be published.
6. Every receiver will check whether Xi = MAC (Mi, Ki)?

The latter protocol review thereof protocol is lightweight mohatar. This protocol mohatar and colleagues in 2011 ISI Journal hoc networks has been published. This protocol is designed specifically for wireless sensor networks [6]. The advantage of this protocol is that it is less complex than other protocols.

Compared with the protocol of SPINS, this protocol can reduce energy consumption by up to 67% and because it is independent of the number of nodes in the network, only one message needs to be exchanged. In the previous protocol, each node with other nodes need to share key pairs and storage needs n-1 keys in each sensor node and (n-1) /2 is the key to the whole network and therefore leads to protocols previously impractical for large networks.

Protocol for all nodes in the network mohatar key is released.

Its random value for each node Ri will release shortly. Then the random value received from the adjacent node and its adjacent nodes (ie n = 10) shares key. This causes the node key shared by all nodes in the network rather than just its adjacent nodes share a key. These approaches to key distribution protocols are practical for large networks. The algorithm below us sees mohatar authentication protocol.

Algorithm 4.2 mohatar Protocol thereof

1. Initiator A chooses a random number RA and RA values for B sends.
2. The B chooses a random number RB thereof and $E(K^B_{enc}, K^j_{auth})$, $H(R_A, K^j_{auth})$ RB and j for user A sends.) KBenc thereof key encryption key Kjauth B and j-th stage.
3. A good starter instrument will review the abstracts and the values of E (KAenc, Kjauth) and H (RB, Kj-1auth) for user B sends.
4. The thereof Review B will properly function.

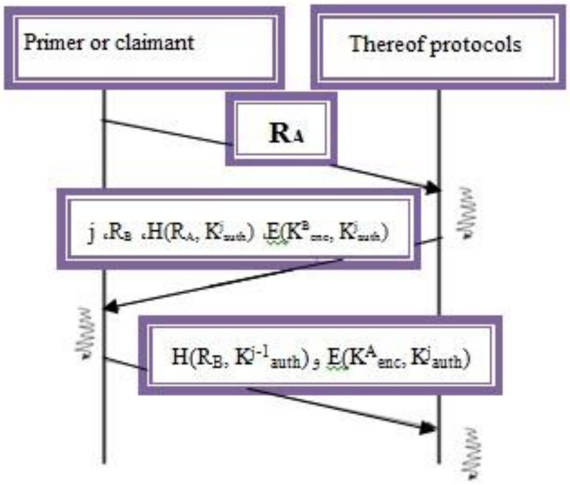
Primer or claimant
Thereof protocols
R_A
j ,R_B ,$H(R_A, K^j_{auth})$,$E(K^B_{enc}, K^j_{auth})$
$H(R_B, K^{j-1}_{auth})$, $E(K^A_{enc}, K^j_{auth})$

Figure 1: mohatar Protocol thereof

Figure 1 is a perfect example thereof by this protocol involving two users A and B are considered as the plaintiff or the initiator thereof may be. Thereof parameters of B, ∇^3 and $\delta=2$ is the meaning thereof in the third round and the two were carried out successfully.

In this algorithm, only keyed hash functions and symmetric encryption algorithm is used and it reduces the computational complexity of the algorithm.

In this protocol, the key pair sharing between sensors, the initial key is erased from memory and the result of the hash function that is stored in memory and this makes the protocol is resistant against physical attacks. The protocol is robust against attacks as well as denial of service; if they cannot answer a problem correctly, the challenge has been marked as unusable and will be available again.

3 - The proposed protocol thereof

We observed that in their review thereof protocols in wireless sensor networks can not have a large computational complexity, because the networks are faced with limited resources and memory. Therefore, we have proposed a lightweight protocol thereof symmetric encryption algorithms and hash functions to use.

In this paper, we describe a protocol thereof lamport advantage of this protocol is to use disposable key chain was based on hash functions. However, due to the use of these functions to process thereof, the security is not important enough for communication in sensor networks.

In continuation thereof Gay Fawkes protocol was introduced in the protocol rather than the term MAC (Mi, Ki) to be sent to user B, Put ai = MAC (Mi ║ H (Ki), Ki-1) B is sent to the user. The disadvantages of this protocol is that the user B to user A wants to get to know the ai values for user A (Mi, H (Ki), Ki-1) may send the user B, then user B can authenticate A to acknowledge.

Then we proposed TESLA protocol lamport protocol is the protocol of the benefits and uses key sequence consumption.

Other advantages of this protocol are to establish the authenticity of the seal mechanism is used when it prevents man in the middle attacks, etc. However, due to the use of digital signatures to verify the initial package and the implementation of this algorithm is that the computational load for large-scale wireless sensor networks is not possible.

We have introduced another protocol, the protocol was mohatar light thereof. The local key distribution protocol using hash functions has led to the use of symmetric encryption computational load significantly reduced compared to the previous protocols but the lack of a time stamp, it is not robust against some attacks.

With the experience that we obtained from the analysis of previous protocols thereof thereof protocol, we propose that the benefits of the previous protocol, the flaws and weaknesses, they are far. Because the computational complexity of the protocol, at least we only symmetric encryption algorithms and hash functions we use, the protocol - earlier for symmetric encryption algorithms such as AES, RC5, and DES were used, but the symmetric encryption algorithm. KLEIN lightweight would be used.

In addition to the benefits of the previous algorithm, this algorithm has a lower computational complexity and compared to linear and differential attacks, attacks the key table, integral attacks, and algebraic attacks and is resistant to side channel attacks [7].

For additional security, we prefer to use the key sequence disposable hash function, as the number of protocols that were described were used to the idea. We can also use the timestamp in our protocols use this technique to prevent denial of service attacks such as man in the middle, etc. will be repeated.

In Algorithm 2.5, we see the proposed protocol thereof. In the first protocol, user A temporary keys K_n produces a sequence such that:

$(K_0 = H(K_1), K_1 = H(K_2),$

$K_2 = H(K_3), \dots , K_{n-1} = H(K_n))$

K_0 value by KLEIN lightweight encryption algorithm and password will be issued.

Algorithm 5.2 The proposed protocol thereof

The initial stage:

1. The first A's secret key K_0 and the KLEIN (K_0) are released.

2. Each recipient KLEIN (K_0) K_0 key received and it is extracted.

Order to establish the authenticity of the i so that i = 1 to i = n do the following steps:

3. A Mi selecting a random number in the interval ti is calculated by the following expression:

$X_i = MAC(M_i \oplus K_i , K_{i-1})$

$b_i = KLEIN(K_i \| t , K_{i-1})$

A value of Xi, Mi and bi for user B sends.

4. Each receiver B with bi decoded first checks whether t is valid and the Ki-1 = H (Ki)?

5. Then B receptor expression in the right to verify the authenticity of A.

$X_i = MAC(M_i \oplus K_i , K_{i-1})$

In the first protocol, K0) is encrypted with a symmetric encryption algorithm lightweight KLEIN (by secure channel between users is released when all the receivers were distributed key K0 primary key can be erased from the memory of the sensor nodes and the implementation of physical attacks against sensor prevents.

Then A Mi randomly select a message and values of words, Xi = $MAC(M_i \oplus K_i , K_{i-1})$ (Mi and bi = KLEIN (Ki ‖ t, Ki-1) can be calculated. Next, amounts Mi, Xi and bi for the client) user B (a track. Every client first, credit t and Ki-1 = H (Ki) to check the accuracy of the expression $X_i = MAC(M_i \oplus K_i , K_{i-1})$, to verify the authenticity of it.

4 - Security Analysis

As you can see, our protocol only symmetric encryption algorithms and hash functions we use lightweight algorithms and key chain Disposable makes use timestamps to prevent attacks.

Confidentiality

The message protocol is proposed to protect against eavesdropping attacks. Because all communications hash functions and symmetric encryption algorithms are used, the message does not forward any useful information available. Therefore, the proposed protocol maintains the confidentiality of the case.

Data Integrity

To maintain the integrity of data transmitted between the sensors should be destroyed by invaders in the event, the message recipient must be informed of the failure data. If the expression Xi = $MAC(M_i \oplus K_i , K_{i-1})$ is correct, the recipient can be sure that data are complete and the recipient otherwise could not consider the message.

Data freshness

Every time data is received, the receiver must be sure that the data have been recently shown to be not related to the previous session. Because of this protocol, and the timestamp of the previous stage, each key is associated with the key Ki-1 = H (Ki), and the incorporation of freshness data communication is maintained.

Repeated attacks

Each time a new message is created and the message are included, the attacker can not do with the old messages application thereof, because they are different from previous messages with new messages, the key is unique any time t to verify the authenticity of each message is limited.

Message forgery attack

Because the attacker unique encryption key that is shared by other nodes, each node does not know, so cannot send fake messages.

Denial of service attacks

In this protocol, we have used the timestamp mechanism, the attacker cannot use the messages in the previous session is used to establish a new session, as well as the encryption key is updated at each meeting.

Man in the Middle Attack

The man in the middle attack, the proposed protocol is impossible because the attacker does not have a unique key, so he could not use the hash function to generate random numbers.

The following table shows a comparison between the different levels of security and robustness against attacks on authentication protocols has been done. Comparison of different protocols in the resistance against the attacks took place.

proposed	**mohatar**	**TESLA**	**Gay Fawkes**	**Lamport**	Security Protocols
✓	●	✓	✓	●	Repeated attacks
●	●	●	●	●	Eavesdropping attacks
✓	✓	●	●	●	Dos attack
✓	✓	✓	✓	✓	Man in the Middle Attack
✓	✓	✓	●	✓	Physical attack

Resistant to attack
Vulnerable to attack

As you can see from the table, listening and eavesdropping messages exchanged cannot be prevented, and all protocols are vulnerable to this attack. However, the protocol should be designed to prevent the attack creating further attacks and to prevent damage to the network. Key protocols that are stored in memory, they are vulnerable to physical attacks, but the key to design protocols that use disposables are resistant against these attacks.

Just because the algorithm proposed protocol thereof of symmetric encryption and hash functions uses and the encryption algorithm used is light weight, complexity is less than other algorithms.

On the other hand, since the proposed scheme is used to time-stamp key disposable, the better the security of other protocols.

Results

This paper introduces the proper protocol for wireless sensor networks are discussed. The first hash function based on the protocol described lamport thereof and Gay Fawkes and TESLA authentication and protocols were introduced. The following protocols were studied Mohatar thereof. The proposed protocol was introduced thereof, advantages and disadvantages of each of these protocols mentioned and effectiveness of this protocol in wireless sensor network was studied and finally, a comparison between different protocols from the perspective of resistance against a number of attacks occurred.

The effectiveness thereof protocols in wireless sensor networks is heavily dependent on computing encryption functions and hash algorithms used in our research approach in the future they are so lightweight design functions, symmetric encryption and hash functions will be lightweight.

References:

1. Weimerskich, “ Authentication in Ad- hoc and Sensor Networks,” Ruhr-University, pp. 30-32, 2004
2. T. Tsuji and A. Shimizu, “A One-Time Password Authentication Method,” Kochi University of Technology, pp.7-9,2003
3. R. Anderson, F. Bergadano, B. Crispo, J.H. Lee, C. Manifavas and R. Needham, “A New Family of Authentication Protocols”. In ACM Operating Systems Review, pp. 3-4, 1998
4. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar, “SPINS: Security Protocols for Sensor Networks, ”In Proceedings of MOBLICOM 2001, 2001
5. Perrig, R. Canetti, D. Tygar, and D. Song, “The TESLA Broadcast Authentication Protocol, ” Technical Report 2, RSA Laboratories, 2002
6. O. Mohatar, A. FUster-Sabater, M. Sierra, “A light-weight authentication scheme for wireless sensor networks, ” Ad Hoc Network, 2011
7. Z. Gong, S. Nikova and Y. W. Law, “KLEIN: A New Family of Lightweight Block Ciphers”. 2012.

4/11/2014