International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

September 2014 | Issue 20 | Volume 6 | Number 3 | Pages 1-5

PROPOSING A KEY MANAGEMENT AUTHENTICATION PROTOCOL IN WIRELESS SENSOR NETWORK (WSNS)

B. Kheradmand R. Fekri

Department of Computer Engineering, Parsabsad Moghan Branch, Islamic Azad University, Parsabad Moghan, Iran
behbod@iaup.ac.ir, r_fekri2000@yahoo.com

Abstract- Wireless sensor networks (WSN) use sensor nodes in an unprotected environment in which data are transmitted and received. Data should be transmitted in the encrypted format to prevent the leakage of data by information invaders. For this purpose, encrypting mechanisms should be used. Having secure encryption mechanisms requires using protocols of secure key management. There are many key management protocols which have both strong and weak points. They are vulnerable to attacks. The protocol proposed in this paper is a two-sided key bilateral management protocol for authenticating originality which has asymmetric encryption. The proposed protocol uses nonce and timestamps to ensure that keys and messages are new and prevents the repetition attack. To evaluate the overall security of the proposed protocol, security of the protocol in WSNs was examined. In this study, the proposed protocol was investigated in AVISPA software and the results of the study revealed that the proposed protocol is secure.

Keywords: WSN, Security Evaluation, Key management, Originality Authentication, Key Communication.

I. INTRODUCTION

Wireless sensor networks consist of small autonomous nodes. Each node has a small microprocessor, a radio chip, some sensors, and is usually battery powered which limits network lifetime. Applications of wireless sensor networks run the gamut from environmental monitoring and healthcare to industrial automation and military surveillance [14-15].

Wireless sensor networks (WSNs) were indeed invented to gather data from an insecure and unreliable environment. Radio signals [14] are used to exchange information in WSNs. Attackers are likely to use the same signal and pretend themselves as a member of networks , and hence gain access to information. All the proponents and providers of security protocols for WSNs believe that an invader can take the entire control of a sensor through direct communication.

In order to protect the communicated data in such environments and contexts, one should keep the encryption keys secret. As a matter of fact, key management is considered to be one of the most challenging issues with respect to the security of WSNs. Different protocols of key management have certain merits and drawbacks and they are usually likely to be attacked. In the present study, the proposed protocol aims to minimize the drawbacks and weaknesses of the previous protocols which will be later evaluated and assessed with respect to such attacks.

This paper is organized as follows: In section II, security is described. After that, in section III, the methods and protocols are described. Then, in section IV, the proposed protocol is presented. Then, in section V, the security analysis of the proposed protocol is presented. Finally, in section VI, conclusions of the study are reported.

II. SECURITY IN WSNS

Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, nonrepudiation [16]. The more the dependency on the information provided by the networks has been increased, the more the risk of secure transmission of information over the networks has increased. For the secure transmission of various types of information over networks, several cryptographic and other techniques are used which are well known.

Wireless sensor networks use insecure and unreliable contexts and environments to transmit and receive data. However, security in these contexts is considered to be a key criterion and requirement. In particular, in military contexts where security is of high significance, presenting a protocol which takes all the security issues into account is desirable and highly important. Using encryption mechanisms to transmit and receive data is one of the methods of establishing security in WSN contexts. According to this method, having secure encryption mechanisms involves the use of secure encryption keys. Hence, to establish safe and secure encryption keys, one has to use certain protocols for managing the key. Key management protocols should meet specific security and operational requirements. In other words, privacy, accuracy and authentication can be regarded as some of the security requirements of these protocols while scalability, flexibility and accessibility are among the important operational requirements in WSNs which should be taken into consideration in designing key management protocols [2, 5, 6].

III. METHODS AND PROTOCOLS OF KEY MANAGEMENT

In the relevant literature, several different methods and schemes have been proposed by researchers in WSNs to manage key which have their own pros and cons. For instance, reducing the memory space and computational load in Eshenauer [2], reducing communication load, enhancing flexibility and authentication of nodes before transmitting data in leaps [2], authenticating the originality of nodes before transmitting data in PKMV2 [1], improving strength and robustness in Q-composite [4] are the major advantages and merits of the protocols which have been presented in the relevant literature.

However, weakness in repetition attack in leap, weakness in repetition attack and individual attack in PKMV2 are among the shortcomings of the main protocols which should be addressed and resolved in designing new protocols. Table 1 gives an outline of the key management protocols [2, 4, 7, 9, 10, 11, 12, 13].

Table 1. An outline of the designs for managing key [2]

Design	Description
Eshneuver	Random number of keys (K) are selected randomly from a big reservoir and form a key ring. Shared keys are allowed to communicate in a pair of key rings related to the nodes.
q-composite	Random number of keys (K) are selected from a reservoir and form a key ring. Q is selected as a shared key in a pair of key rings related to the node and are allowed to communicate.
Daewoo	T matrix of keys are selected and using matrix multiplication, shared and paired key is calculated dynamically.
Leap	A pre-distributed k is used to record four types of keys.
Yener	It uses combinatory design of BIBD to distribute keys.
Shell	It uses a distributed key management entity to produce and manage keys.
Panja	Several minor keys are used to calculate group keys dynamically.
Yang	It uses a key-integrating function to calculate key in any session.

IV. THE PROPOSED PROTOCOL

The key management protocol proposed in this paper is a bilateral authentication protocol which has asymmetric encryption. The original idea of this protocol has been adapted from PKMV2; however, unlike PKMV2 in which symmetric encryption was used, in the proposed protocol asymmetric encryption was used. The given protocol is as follows:

0. shared public key k_{UA}, k_{UB} between A, B saved in database A, B

1. $A \rightarrow B: k_{UA}, A, MAC_k\{k_{UA}, A\}$

2. $B \rightarrow A: k_{UB}, B, MAC_k\{k_{UB}, B\}$

3. $A \rightarrow B: E_{k_{UB}}(r_1, A)$, 4. $B \rightarrow A: E_{k_{UA}}(r_1, r_2)$

5. $A \rightarrow B: E_{k_{UB}}(k_s), E_{k_s}(r_2, t_A, l)$, 6. $B \rightarrow A: E_{k_s}(r_1)$

The features of this protocol is illustrated in Table 2.

Table 2. The used features in the proposed protocol

General key A	k_{UA}	Nonce produced by B	r_2
General key B	k_{UB}	ID A,B	A, B
Nonce produced by A	r_1	Timestamp A	t_A
Communicated key	k_S	Validity time span for general and special temporary key A	l

In the first stage of the proposed protocol, node A transmits its general key and ID as well as MAC value to node B. In the second stage, node B transmits its general key and ID as well as its MAC value to node A. In the third stage, node A produces a random number and creates an encryption with general key B and its ID and transmits it to node B. In the fourth stage, node B produces a random number and creates an encryption with the random number received from node A and then transmits it to node A. In this stage, the two nodes authenticate one another and then communicate keys with each other. In the fifth stage, node A transmits the value $E_{k_{UB}}(k_s)$, $E_{k_s}(r_2, t_A, 1)$ to node B. In the sixth stage, node B transmits $E_{k_s}(r_1)$ to node A to acknowledge that it has received message five. In this protocol, the two nodes authenticate each other in four stages and then they start to communicate keys with each other during the next stages.

V. SECURITY ANALYSIS OF THE PROPOSED PROTOCOL

In this section of the paper, the proposed protocol will be analyzed with respect to the attacks and security features and characteristics. The security analysis of the protocol will also be carried out using AVISPA software.

A. Evaluating the Proposed Protocol in Terms of Security Features

The following security features and attacks related to the WSNs will be discussed here in the following order:

A.1. Authentication

When two sides want to maintain meeting sessions with each other, they need a private key for the session. In order to communicate the meeting key, the two sides should go through four stages so as to first authenticate each other and prove their originality to one another. Having gone through these stages, the two sides send the session key to one another with confidence. In many other protocols which has been presented in the literature, authentication was carried out in a one-way and unilateral manner and hence the authenticity of the other side could not be acknowledged.

As a result, the probability of individual attack was high in those protocols. The bilateral and two-sided authentication put forth in this protocol can sort out this thorny issue. Earlier protocols such as Eshenauer, q-composite and yener lack the node authentication stage. In contrast, this significant feature is fulfilled in the proposed protocol.

A.2. Confidentiality of Data

Encryption algorithms need to be used to ensure the confidentiality of data. Secure and reliable encryption algorithms call for using secure encryption key. Consecutively, there is a need for a secure key management protocol. Since asymmetric encryption has been used in this study and asymmetric encryption is more secure, it can be argued that the security criterion is met for the proposed protocol. However, earlier protocols used symmetric encryption in which there was only one encryption and decryption. Hence, in case it is disclosed, the security and confidentiality of data will be threatened. Nevertheless, inasmuch as two general and special keys are used for encryption and decryption in this protocol, the security and confidentiality of the data will be ensured.

A.3. Resistance to Forge and Fake

In order to fulfill a fake attack, the ID of the invader should be able to acquire the confidential values for forging. However, the confidential values are not transmitted overtly in the proposed protocol; rather, they are transmitted in the encrypted and signed manner. Thus, due to the lack of special key, the invader cannot easily detect the confidential values. This hinders and prevents the forging and fake by the invaders. Nevertheless, the earlier protocols did not possess this feature and they used symmetric encryption. As a result, the security of the data was not completely protected in previous protocols.

A.4. Resistance to Repetition Attack

Inasmuch as the two sides involved in message production use random numbers, repetition attack is not likely in this protocol and even if repeated messages are transmitted, the invader will not be able to get informed about the next sessions. This is due to the fact that asymmetric encryption is used in this protocol and the invader does not possess a special key decrypt the received message.

A.5. Resistance to Man in the Middle Attack

Unlike the proposed protocol, the majority of available protocols in the related literature are vulnerable to a man in the middle attack since they do not authenticate the nodes. This leads to the susceptibility of protocols against this attack. In the proposed protocol, nonce random values and bilateral authentication are used which eliminates this weakness. Regarding attack a man in the middle, the invader should be able to decrypt the received message which is highly difficult due to the use of asymmetric encryption general and special keys.

Moreover, the invader cannot understand the results of authentication since the authentication messages can only be read by the two respective sides and the others cannot read the messages even if they get access to them. Thus, it can be mentioned that the proposed protocol is secure against these attacks.

B. Evaluating the Protocol Using AVISPA Software

This software is regarded as one of the specific tools used for analyzing security protocols. In this software, protocol is analyzed completely automatically.

This software receives a high-level description of the protocol and its intended purposes and then illustrates and depicts the state of the protocol with regard to the presence of the invaders. Next, the tool reports the probability of fulfilling the security goals. In case the protocol fails, the software illustrates the attack pattern. In this tool, it is possible to evaluate the protocol on the basis of the user's unique intentions and the entire process of detecting the accuracy and attack pattern can be carried out.

The protocols which are examined by this tool are described by the HLPSL language which is a simple and role-oriented. This language is capable of describing and modeling the protocol and expressing the security goals. All the data and control structures and the security requirements can be described in this language. Although asymmetric encryption protocol requires high computational capability, it uses two general and special keys for encryption and decryption and hence it is more secure than the symmetric encryption. Using the produced random nonce number by both sides acknowledges the novelty and originality of the key.

In some security protocols, a third reliable party is used to communicate the key. The third party requires additional memory to store the received keys. Since the proposed protocol does not use a reliable third party, it does not have the bottleneck problem of the third party. If the simultaneity issue is resolved, the proposed protocol will have higher efficiency and security than other protocols.

The investigation of the security of the protocol was carried out through operationalizing the attacks on the protocol and acknowledged the failure of the attacks. For example, regarding man in the middle attack on this protocol, message is encrypted by general key B in the third stage and decryption is carried out only by special key B and it is only node B which has access to the special key. Thus, even if the invader receives the message, it cannot decrypt the message. As a result, the attack ends in failure.

Also, reflection attack on this protocol is unsuccessful and fails. If the invader starts the attack, the performing time of the protocol might be finished and as a result of key expiration time and date, the invader will fail. In the PKMV2 plan which is the underlying and basic idea for the protocol, using the symmetric encryption and awareness of everybody of the key makes it weak and vulnerable to repetition attack and a man in the middle attack. This weakness and drawback has been eliminated by using asymmetric encryption in the proposed protocol.

The conducted analysis and investigation acknowledges the security of the proposed protocol. Also, as the results of the analysis show, the resistance of this protocol to the common attacks in key management protocols has been proven. Some of these common attacks include node capture attacks, violation of data privacy, forging attack and repetition attack. Furthermore, the proposed protocol has two-sided and bilateral authentication and uses asymmetric encryption. Hence, this protocol is resistant to the man in the middle attack.

In order to analyze the security of the protool, the researcher used the AVSIPA software. This software is a formal method for examining and analyzing the security and safety factor of protocols. The proposed protocol has been written by the HLPSL language. Moreover, Attacks were simulated on the protocol to investigate the security or insecurity of the protocol. The analytical output of the protocol by the AVISPA software and the safe results of this software indicate the safeness and security of this protocol. The followings show the results:

```
 %OFMC
 %Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\progra~1\SPAN\testsuite\results\pkm2.if
GOAL  as_specified        BACKEND
  OFMC
COMMENTS                  STATISTICS
  parseTime: 0.00s
  searchTime: 0.03s  visitedNodes: 27 nodes  depth: 8 plies
```

VI. CONCLUSIONS

WSNs make use of sensor nodes in unprotected environments. As a result, safety and security is considered as a high priority in these networks. One of the methods of establishing safety is to use encryption which is made possible by using encryption keys. The security of encryption algorithms depends on the security key. Thus, these keys should be properly handled so that safety can be maintained. The earlier protocols used symmetric encryption which has lower safety than the asymmetric encryption. The protocol presented in this paper was based on asymmetric encryption. The results of the safety analyses and investigations conducted in the present study revealed that the given protocol is resistant to attacks. It is recommended that interested researchers use reliable and accurate methods for analyzing and investigating key management protocols in WSNs.

REFERENCES

[1] A. Sarmast, M.A. Ashra, M.R. Meybodi, "Provide a Key Management Protocol in Wireless Sensor Networks", National Conference on Information Security and Communications, Ahvaz, Iran, 2010.

[2] L. Eshenauer, V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks", 9th ACM Conf. Comp. and Commun. Sec., ISBN: 1-58113-612-9 Order Number: 537020, New York, USA, Nov. 2002.

[3] M. Younis, K. Ghumman, M. Eltoweissy "Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks", IEEE Trans. Parallel and Distrib. Sys., Vol. 17, Issue 8, pp. 865.82, August 2006.

[4] H. Chan, A. Perrig, D. Song, "Random key Predistribution Schemes for Sensor Networks", Symposium on Security and Privacy, IEEE Computer Society, pp. 197-213, Washington, DC, USA, May 2003.

[5] W. Du, et al., "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks", ACM Transactions on Information and System Security (TISSEC), Issue 2, Vol. 8, pp. 228-258, , New York, USA, May, 2005.

[6] M.K. Joseph, H.K. Randy, S.J.P. Kristofer, " Emerging Challenges: Mobile Networking for Smart Dust", IEEE Journal of Communications and Networks, Issue 3, Vol. 2, pp. 188-196 , September 2013.

[7] Y. Chevalier, et al., "A High Level Protocol Specification Language for Industrial Security-Sensitive Protocols", Proc. SAPS. 4, pp. 193-205, Austria, 2005.

[8] S.A. Camtepe, B. Yener, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks", Comput. Sci. Dept., Rensselaer Polytech. Inst., Issue 2, Vol. 15, pp. 346-358, Troy, NY, USA, April, 2007.

[9] P. Kumar, V. Kumar, "A Key Management Protocol for Hierarchical Wireless Sensor Networks", International Journal of Computer Science & Engineering Technology (IJCSET), Issue 2, Vol. 4, pp. 124-130, Feb. 2013.

[10] Y. Cheng, P. Dharma, "An Improved Key Distribution Mechanism for Large Scale Hierarchical Wireless Sensor Networks", Elsevier (Security Issues in Sensor and AD HOC Networks), Issue 1, Vol. 5, pp. 35-48, January 2007.

[11] A. Armando, et al., "The AVISPA Tool for the Automated Validation of Internet Security Protocols and Application", 17th International Conference on Computer Aided Verification, Lecture Notes in Computer Science, LNCS 3576, pp. 281-285, Berlin, Germany, 2005.

[12] S. Ozdemir, et al., "Performance Evaluation of Key Management Schemes in Wireless Sensor Networks", Journal of Science, Gazi University, Issue 2, Vol. 25, pp. 465-476, Ankara, Turkey, 2012.

[13] B. Panja, S.K. Madria, B. Bhargava, "Energy and Communication Efficient Group Key Management Protocol for Hierarchical Sensor Networks", IEEE Int. Conf. Sensor Networks, Ubiquitous, and Trustworthy Computing, Vol. 1, pp. 384-393, Taichung, Taiwan, June 2006.

[14] B. Kheradmand, L. Mohammadkhanli, "Enhancing Energy Efficiency in Wireless Sensor Networks via Improving Elliptic Curve Digital Signature Algorithm", World Applied Sciences Journal, Issue 21, Vol. 11, pp. 1616-1620, 2013.

[15] H. Barati, A. Movaghar, A.M. Rahmani, A. Sarmast, "A Distributed Energy Aware Clustering Approach for Large Scale Wireless Sensor Network", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 13, Vol. 4, No. 4, pp. 125-132, December 2012.

[16] A.S.K. Pathan, et al., "Security in Wireless Sensor Networks: Issues and Challenges", 8th International Conference on Advanced Communication Technology (ICACT), ISBN 89-5519-129-4, Vol. 3, Korea, Feb. 2006.

BIOGRAPHIES

Behbod Kheradmand was born in Parsabad Moghan, Ardabil, Iran in 1985. He received the B.Sc. and the M.Sc. degrees both in Software Engineering from Islamic Azad University, in 2006 and 2011, respectively. Currently, he is a Lecturer and Academic Member in the field of Software Engineering at Parsabsad Moghan Branch, Islamic Azad University, Parsabsad Moghan, Iran and teaches software engineer, operating system, and C# programming. His research interest is in the area of security in network.

Roggayeh fekri was born in Parsabad Moghan, Ardabil, Iran in 1985. He received the B.Sc. and M.Sc. degrees in Computer Engineering and Software Engineering and IT from Jahad Daneshgahi and Malek Ashtar University, Iran in 2008 and 2013, respectively. Currently, she is a lecturer of Software Engineering at Parsabsad Moghan Branch, Islamic Azad University, Parsabsad Moghan, Iran and teaches operating system, and C# programming. Her research interest is in the area of security in network.