Volume: 08 Issue: 05 Pages: 3209-3212 (2017) ISSN: 0975-0290

Markle Tree Based Authentication Protocol for Lifetime Enhancement in Wireless Sensor Networks

Mallikarjunaswamy N J [1]
Assistant Professor, S.I.E.T, Tumkur
Research Scholar,
Visvesvaraya Technological University, Belgaum,
mallikarjuna2010@gmail.com
Latha Yadav T R [2]
Assistant Professor, A.I.T, Tumkur
Research Scholar,
Visvesvaraya Technological,University, Belgaum,
chethusavi3@gmail.com
Dr. Keshava Prasanna [3]
Professor, Dept of CSE,
C.I.T, Gubbi,
Tumkur
keshava2011@rediffmail.com

ABSTRACT

Wireless sensor networks are self organized, autonomous, automatic discovery of services, highly scalable, reliable, Infrastructure less service. Mainly applicable in the field of disaster, healthcare. The cryptographic operations such as hash based schemes are more energy consuming (more byte transmitted indirectly consumes more energy). To avoid the energy consumption over a cryptographic operations are design of Markle Tree Based Authentication protocol for Lifetime enhancement in wireless sensor networks called MALLI, which uses a famous structure of hash algorithm. To demonstrate that, the default hash tree and the security achieved by the proposed method are more effective than the existing methodologies.

Keywords – **Authentication, Cryptography, Hash function, Security, Wireless Sensor Networks (WSN).**

Date of Submission: March 07, 2017 Date of Acceptance: March 15, 2017

I. Introduction

Wireless sensor network(WSN) is an Adhoc like infrastructure less network that work like self organizing, self healing, autonomous, each and every node cooperate with each other. sensor nodes are unattended devices that are severely constrained in terms of processing power, memory size and energy levels and tradeoff between security and energy consumption are major concerns for all application.

Since WSN are resource constrained networks, we propose a pragmatic approach where we try to balance these two opposing design elements: security and energy. We evaluate our proposal achieve more energy efficient compare to previous.

Code dissemination protocol (eg., MNP[1], MOAP[2], Deluge[3], Freshet[4], Sprinker[5], Strean[6]) have been improved recently to propagate code images using the wireless network created by the wireless nodes. Originally these proposed protocols generally will not give any security without using a hash function. In this, common question raises is that, how we apply hash function to the piece of data which traverse throughout the network widely. assume well-behaves (i.e.,non malicious) sensors of all the reprogramming protocol in the literature Deluge[6] is the benchmark. Also it has been included in the tinyOS distributions.

In order to provide authentication to the entire data is normally based on signature of hash tree. The generating hash tree signature is of two types, one is by using chain operation and other is markle tree. To generate hash chain, each packet gives its hash value to its upstream packets until to reach end of packet with the signature. As in markle tree each packet generates its own hash value independently and produces hash tree with the signature (top of the node).

In the recent years much progress has been made in the design of practical one way hashing algorithms which is efficient for implementation by both hardware and software. The message digest family which consist of various algorithms such as MD5, SHA1, and 2AMD which produces standard output of 128bit, 160bit and 160bit respectively.

Volume: 08 Issue: 05 Pages: 3209-3212 (2017) ISSN: 0975-0290

Fig 1, States that the previous affairs of message authentication which deals with the balancing nature between security and energy. When security increases along with the energy so challenging task is to provide high security with the minimum energy.

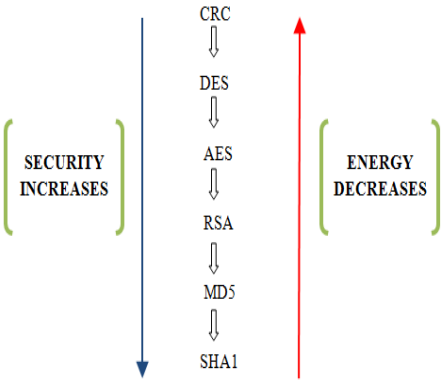

Fig 1: Previous affairs of message authentication

The main purpose of this research is to produce a signature at receiver by using partial hash tree information by the base station and validate the each packet by using one way hashing algorithm of 160 bit output to enhance the security and energy consumption. The proposed paper gives improved version of security with a less execution/run time at receiver end. The result shows that proposed scheme provides better security than the existing one.

This paper is organized as follows: Section II presents the related work and section III presents the proposed methodology. Section IV presents the Experimental analysis. Section V contains the conclusion and future work.

II. Related Work

Wireless sensor networking is a wide technology to observe and extract data from the environment and has an important role in ubiquitous computing. However, these benefits come with various limitations, vulnerabilities, and risks.

To distinguish legitimate data from intruder's data, authentication techniques are frequently used to verify the integrity of the received data in a communication system. There are several message authentication schemes in wireless sensor networks have been proposed. The authentication techniques used in the severely constrained wireless sensor network environments.

Carlos F. et al[7] aims at having a more balanced solution by being more energy conscious, proposing in some instances partial but attack aware solutions. More chance of being adopted in sensor network scenarios needing security in the reprogramming process. Another contribution is that can make evident in energy that radio operations are the most energy consuming operations in update dissemination.

Ayman Tajeddine et al[8] proposed a different authentication techniques suitable for the severely constrained sensor nodes in WSNs, and addressed three main categories based on symmetric cryptography, asymmetric cryptography, and hybrid techniques using both cryptographic methods.

Haider M. AI-Mashhadi et al [9] proposed that the performance of 2AMD-160 improves in increasing of security and time consuming without compromising the security. It is found that the number of message blocks influences the run time of the hash function while the increment in message size only slightly increase the run time.

So, by using the new proposed approach the performance is evaluated and compared with other methods under the same test results to demonstrate the effectiveness of the new approach with regards to enhancement of the run time and security of message in wireless sensor network nodes.

Assumptions

1. The Base station is a powerful entity, with unlimited energy and memory with high frequency range.
2. There is a packet size limit; maximum payload size is 102 bytes.
3. Each sensor node in the network is preconfigured with the minimum energy and memory.

III. Proposed Methodology

The solution we proposed is the image size is divided into equal number of pages and each page is subdivided into equal number of packets.

Apply the hash function for number of packets [10], as shown in fig 2.

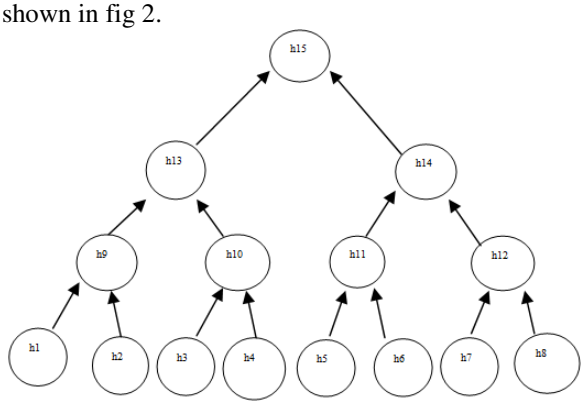

Fig 2. Applying Hash Functions

Generating signature has two types 1) using partial tree information and 2) using hexadecimal addition.

Volume: 08 Issue: 05 Pages: 3209-3212 (2017) ISSN: 0975-0290

In case of partial tree information sender sends the partial information of tree as like h2, h10 and h14. Using partial information receiver can easily generate the signature at receiver side.

h(h(h(h(P1)||h2)||h10)||h14) → Signature at receiver side.

In case of using hexadecimal addition the receiver can generate the signature as shown below format.

h1+h2=h9
h3+h4=h10
h5+h6=h11
h7+h8=h12
h9+h10=h13
h11+h12=h14
h13+h14=h15 → Signature at receiver side

Finally, 160 bit signature is generated. This proposed approach is more effective compare to previous approaches. Existing methodologies proposes either MD5 (which gives output of 120 bits, but 2AMD gives 160 bits) or SHA1 (which gives 80 rounds where as in 2AMD-160 included 64 rounds).

Table 1.key characteristics of 2AMD-160 algorithm[9].

Name	Block size/bits	Word size/bits	Output size/bits	Rounds
MD5 [32]	512	32	128	64
SHA1 [5]	512	32	160	80
2AMD-160	512	32	160	64

IV. Experimental Analysis

The 2AMD-160 methodology enhances the efficient way of encrypting the data in secured environment. In order to encrypt data, SHA1 algorithm uses 0.47 Time/ms to process only the single space, but the new methodology 2AMD-160 takes 0.2 Time/ms of execution time. So, 2AMD-160 consumes less execution time compared to the existing methods such as SHA1, SHA256 and SHA512, which in turn gives the better performance.

Performance Evaluation

In this we evaluate the comparison between chain based hash tree versus markle tree based hash tree in terms of packet verification, packet receiving at destination node, size of the signature in terms of bits.

Table 2. key characteristics of Hash tree.

Hash tree	Packet verification	Packets receive at destination	Signature (size)
Chain based	Dependent	Sequential	160 bit
Markle tree	Independent	Random	160 bit

V. Conclusion

The proposed system message authentication enhances security with light weight hash function at the receiver node; the default hash tree balances security and provides independent packet verification with 160bit signature and authenticates every packet by using 2AMD-160 algorithm. The proposed scheme ensures that markle tree is more efficient then chain based hash. The performance evaluation result shows that the proposed scheme is effective and scalable.

Future work

We are planning to propose new algorithm for better encryption and decryption method for message authentication.

References

[1] S. Kulkarni, and L. Wang, “MNP: Multihop network reprogramming service for sensor networks”, Proceedings of the 25th IEEE International Conference on Distributed Computing Systems, Columbus Ohio USA, pp. 7-16, Jun 2005.

[2] T. Stathopoulos, J. Heidemann, and D. Estrin, "A remote code update mechanism for wireless sensor networks", CENS Technical Report 30, University of California UCLA, 2003.

[3] J. Hui, and D. Culler, “The dynamic behavior of a data dissemination protocol for network programming at scale”, Proceedings of the 2nd international conference on Embedded networked sensor systems, Baltimore MD USA, pp. 81-94, Nov 2004.

[4] M. Krasniewski, R. Panta, S. Bagchi, C. Yang, and W. Chappell, “Energy-efficient on-demand reprogramming of large-scale sensor networks”, ACM Transactions on Sensor Network, 4(1):1-38, 2008.

[5] V. Naik, A. Arora, P. Sinha, and H. Zhang, “Sprinkler: A reliable and energy efficient data dissemination service for wireless embedded devices”, Proceedings of the 26th IEEE International Real-Time Systems Symposium, Miami Florida USA, pp. 277-286, Dec 2005.

Volume: 08 Issue: 05 Pages: 3209-3212 (2017) ISSN: 0975-0290

[6] R. Panta, I. Khalil, and S. Bagchi, "Stream: Low overhead wireless reprogramming for sensor networks", 26th IEEE International Conference on Computer Communications, pp. 928-936, 2007.

[7] Ayman Tajeddine Ayman Kayssi Ali Chehab Imad Elhajj, "Authentication Schemes for Wireless Sensor Networks "Proceedings of 17th IEEE Mediterranean Electro technical Conference, Beirut, Lebanon, 13-16 April 2014.

[8] Carlos F. Caloca de la Parra, J. Antonio Garcia-Macias," A Protocol for Secure and Energy-Aware Reprogramming in WSN", Proceedings of 2009 International Conference on wireless communications and mobile computing connecting the world wirelessly.

[9] Haider M. AI-Mashhadi, Hala B. Abdul-Wahab , Iraq Rehab F. Hassan ," Secure and Time Efficient Hash-based Message Authentication Algorithm for Wireless Sensor Networks" Proceedings of IEEE,978-1-4799-5627-2/14, 2014.

[10] Lin Xu, Hala Mi Wen, Jinguo Li," A Bidirectional Broadcasting Authentication Scheme for Wireless Sensor Networks" Proceedings of IEEE,978-1-5090-0089-0/15, 2015.

[11] I. S. Alshawi, L. Van, W. Pan and B. Luo, "Lifetime enhancement in wireless sensor networks using fuzzy approach and A-star algorithm," IEEE Sensors J., vol. 12, no. 10, pp. 3010-3018, Oct. 2012.

[12] Trevatha.l., Ghodosi H., and Myers T., "Efficient batch authentication for hierarchical wireless sensor networks," in IEEE ISSNIP, pp. 217-222, 2011.

Biographies and Photographs

Mallikarjunswamy received BE from Visvesvaraya Technological University and M.Tech in computer science and engineering in the year 2011 and pursuing Ph.D in VTU. Teaching and Academic experience of 5 years. Life membership in Indian Society for Technical Education.

Latha Yadav T R received BE from Visvesvaraya Technological University and M.Tech in Digital Electronics in the year 2013 and pursuing Ph.D in VTU. Teaching and Academic experience of 3.5 years.

Dr. KeshavaPrasanna received B.E from Bangalore University and M.Tech in Information and Technology in the year 2005 and Ph.D from Tumkur University in the year 2014. Teaching and Academic experience of 14 years. Life membership in Indian Society for Technical Education (ISTE).