Volume: 07 Issue: 06 Pages: 2963-2966 (2016) ISSN: 0975-0290

Message Authentication Protocol for Lifetime Proficient Hash Based Algorithm 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 Message Authentication protocoL for Lifetime enhancement In wireless sensor networks called MALLI, which uses a famous structure of hash algorithm 2AMD-160. To demonstrate that, the execution time and the security achieved by the proposed method are more effective than the MD5 and SHA1.

Keywords: **Authentication; Hash function; Cryptography; Security; Wireless Sensor Networks (WSN)**

Date of Submission: May 25, 2016 Date of Acceptance: June 20, 2016

I. Introduction

Wireless sensor network(WSN) is an Adhoc like infrastructure less network that work like self organizing 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 resource consumption. 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. These proposed protocol generally 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 secure the message transmission confidentiality measures such as encryption, decryption. On the other side, authentication allows entities to validate the integrity of message and also verify the confidentiality of the communicating devices.

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 MD2, MD4, MD5 and SHA family which produce 160,256,384,512 bit.

The main purpose of this research is to produce a secure one way hashing algorithm of 160 bit to enhance the security and energy consumption. The proposed paper gives improved version of security with a less execution/run time. The more security depends on the length of MD generated by the hash functions which is limited by the size of input to the algorithm. 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

Volume: 07 Issue: 06 Pages: 2963-2966 (2016) ISSN: 0975-0290

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.

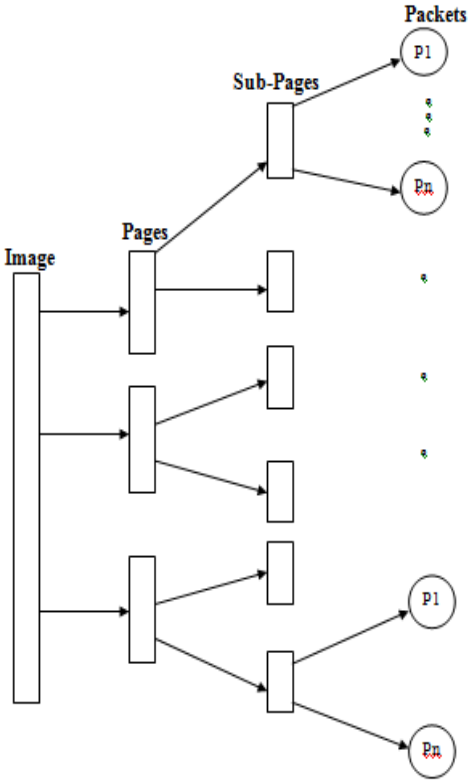
So, by using the new proposed approach the performance is evaluated and compared with other methods under the same test results to demonstrate the effectiveness of the new approach with regards to enhancement of the run time and security of message in wireless sensor network nodes.

Assumptions

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

III. Proposed Methodology

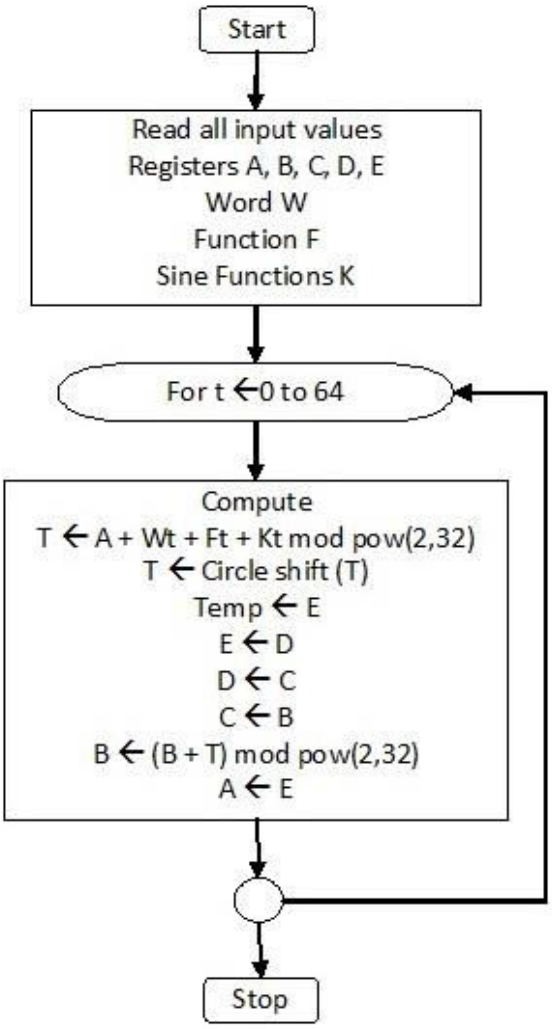
The solution we proposed is the code size of 32bytes that is divided into 8 byte pages and each page is subdivided into 4 byte subpages. Then subpages divided into packets with maximum size of 512 byte as depicted in figure 3.1(a). Output generation for each packet, as shown in figure 3.1(b).



3.1 (a) Generation of Packets

The figure 3.1(b) shows the steps in output generation. It reads all the input values word, function F, Sine functions K and all registers A to E. The word generation process repeats in a loop of 64 iterations. Fist it computes the value of T using Wt, Ft and Kt values, then performs circular shift over the value of T. It changes the value of registers ”A” with ”E”, ”E” with ”D”, ”D” with ”C”, ”C” with ”B” and ”B” with sum of ”B and T”. These values are further processed in update registers phase to generate the digest.

Volume: 07 Issue: 06 Pages: 2963-2966 (2016) ISSN: 0975-0290

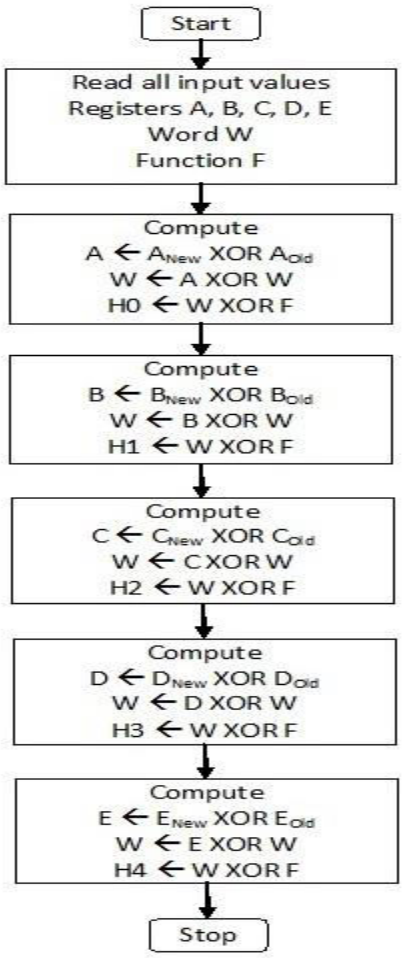


3.1(b) Output Generation

This proposed approach is more effective compare to MD5 (which gives output of 120 bits, but 2AMD gives 160 bits) and SHA1 (which gives 80 rounds where as in 2AMD-160 included 64 rounds).

Update Values

Figure 3.1(c) shows the steps how the registers are update the values. It reads all the registers along with word and functions as parameters. The register H0 is computed using XOR value of W and F, where W is XOR value of register A and W again A is XOR value of Aold and Anew values. Similarly the register H1, H2, H3 and H4 computed using the registers B, C, D and E respectively.



3.1(c) Output Generation

Table 1. key characteristics of 2AMD-160 algorithm

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, MD5 algorithm uses 0.245172ms, but the new methodology 2AMD-160 takes 0.1932159ms of execution time. So, 2AMD-160 consumes less execution time compared to the existing methods such as MD5, SHA1, SHA256 and SHA512, which in turn gives the better performance.

Volume: 07 Issue: 06 Pages: 2963-2966 (2016) ISSN: 0975-0290

Performance Evaluation

The main statement hashes all 10,000 entries one by one. This statement executes 1000 times in a loop, which repeats 3 times execution time in seconds is available.

Table 2. Dissemination time of different hashing algorithms

Algorithms	Execution time(ms)
MD5	10.275190830230713
	10.155328989028931
	10.250311136245728
SHA1	11.985718965530396
	11.976419925689697
	11.86873197555542
SHA256	16.666245007514536
	21.551337003707886
	17.016510963439991
SHA512	18.33939099311826
	18.11187481880188
	18.085782051086426
2AMD-160	10.245428969018820
	10.334678978126631
	10.645496765343210

V. Conclusion

The proposed system message authentication enhances security with light weight hash function; the default hash tree balances security and energy (more security consumes more energy) and authenticates every packet by using 2AMD-160 algorithm. The proposed scheme ensures confidentiality, integrity, freshness of the data. The experimental analysis and 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.

[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]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.

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

Authors Profile

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 2.5 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).