Enhanced security for non English users of Wireless Sensor Networks

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

ABSTRACT

Wireless Sensor Networks is an infrastructure less, self-configured, reprogrammable, energy-aware network used in various applications. Many networks works on security of data including mainly ASCII values but not the non English end users. BDNA cryptography describes how to encrypt non English patterns but which leads to propagation of more bits transmitted means indirectly consumes more energy in WSN. In this we propose new steps to reduce the transmission of more bytes in the network. This gives high propagation speed in the network with minimum hash overhead.

Keywords - ***BDNA, Sensor Networks, MD5.***

Date of Submission: Dec 28, 2017 Date of Acceptance: Jan 17, 2018

I. INTRODUCTION

WSN is the autonomous, well suited for adhoc type of infrastructure, composes several nodes randomly deployed in the infrastructure. Each node has its own memory, frequency range, battery, synchronization unit, transmitter and receiver, analog to digital converter, sensing unit. Sensor is a device which gather and disseminates various information with a security runs from RSA to SHA [1] family.

Wireless Sensor Network (WSN) comprises of hundreds or thousands of minimal effort hubs which could either have a settled area or arbitrarily sent to screen the earth. WSNs are a pattern of the previous couple of years, and they include conveying an expansive number of little hubs. The hubs at that point sense natural changes and report them to different hubs over adaptable system engineering. Sensor hubs are extraordinary for arrangement in unfriendly conditions or over vast land territories.

Remote systems are powerless against security assaults because of the communicate way of the transmission medium. Moreover, remote sensor systems have an extra helplessness since hubs are frequently put in an unfriendly or risky condition where they are not physically secured.

II. LITERATURE SURVEY

In wireless sensor networks the major issue is to provide the data security. In wireless sensor network data security is presented by authentication, Encryption & Decryption. The security algorithm CRC is very easy to execute but less secure, RSA is also very easy to define but less secure, the AES algorithm provides average security, similarly MD5 [1] and SHA [1] family gives more secure compare to all other algorithms. We mainly concentrate on more security with less number of outputs in terms of bits.

Prajapati Ashishkumar B [2] Wireless sensor networks are the most today's discovery in the area of data processing. It gives various on the web furthermore, on-request benefits for information stockpiling; arrange administrations, stage administrations and so on. Numerous associations are apathetic to utilize sensor benefits because of security issues as the information lives on the base station administrations supplier's servers. To address this issue, there have been a few approaches connected by different specialists worldwide to fortify security of the put away information on distributed system. The Bi-directional DNA Encryption Algorithm (BDEA) [1] is one such information security methods. Be that as it may, the current method concentrates just on the ASCII character set, disregarding the non-English client of the distributed computing. In this manner, this proposed work concentrates on improving the BDEA to use with the encryption and decryption algorithm.

Carlos F [3], Haider M [4], Authentication and integrity are the first security attributes tackled by the first secure reprogramming protocols [3]. In these schemes the first relevant problem was preventing malicious code to propagate in the dissemination and compromising remote nodes.

Remote sensor systems administration is a wide innovation to watch and concentrate information from nature and has an essential part in universal figuring. In any case, these advantages accompanied different impediments, vulnerabilities, and dangers [5], [6].

To recognize real information from gatecrasher's information, verification procedures are much of the time used to confirm the uprightness of the got information in a correspondence framework. There are a few message verification conspires in remote sensor systems have been proposed. The confirmation strategies utilized as a part of the seriously obliged remote sensor organize situations.

Ayman Tajeddine et al[7] 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 [8] 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.

The unpredicted power consumption may leads to reduced battery life which is a great burden in the system. In this paper the authors propose a new transmission algorithm in the system which improves the battery life in the system. It combines fuzzy logic method and an algorithm named A-star. It applies the said method and computes the optimal path to the destination by considering the residual energy remaining in each node in the path and the path with minimum hop-count to route packets to the destination. This method also reduces the burden in re-transmitting the same packets to the destination. This approach is more effective and increase the life time of the system. Compared to other approaches, this method assures twenty five percent extra life time in WSNs.

Trevatha. l., Ghodosi H [9] proposed that it makes use of hierarchical system to compute the efficiency of authentication for the incoming packets. Instead of verifying single packet ones, it combine multi packets in the group forming a batch, and entire batch is processed for authentication and reduces the computation overhead. As it make use of hierarchical system, if any sensor has less computational resources and unable to perform authentication, then it request another node in the hierarchy to do authentication task. This situation solves the problem of utilization of resources like battery energy and storage. This approach makes use of cryptographic has methods to generate signature for each message transmission for authentication and all signatures are authenticated in using batch processing.

M. A. Simplicio, et al., [10] proposed that it focuses this problem and adds a solution by using AEAD protocol. This protocol is more effective since it makes use of small tags and generating these tags consumes less computational resources and battery energy. While compared with other protocols which make use of large tags which may be greater than the size of the block and takes additional resources to compute the tags and adds burden to the system to compute the tags. It also reduces the communication overhead since tags are small size we can accommodate more tags in a single packet while transmission which reduces the bandwidth utilization. Compared to other solutions, which provide security by using huge tags which is more than the block size thus incurs extra overhead in transmitting the tags and it needs extra bandwidth. Thus the proposed protocol provides the security in the system with increased efficiency of the life time of the system.

Y. Shuai, et al., [11] proposes a new key management scheme to provide security in WSNs. It creates the keys and is shared by clusters and these keys are updated regularly. Using a crypto hash function with reduced computation it generates keys. When any sensor wants to send the message to its neighbor it should request the key from its neighbor and use the same key for encrypting the message and send the message. Upon receiving the packet at destination it uses its key to decrypt the message. If any eve droppers want inject a false nodes in the system must authenticated by the cluster and acquire the key from the cluster. Hence, any two nodes within the cluster wants to communicate must have the respective keys from the cluster.

III. PROPOSED WORK

Proposed work carries the detail description of original message, Images, Equations, and any non English Language Unicode, ASCII values, encryption and decryption.

Step 1: original message (Images, any non English Languages)

Step 2: Unicode

Step3: ASCII Value

Step4: Encryption/Decryption (MD5 algorithm)

Original message: message is the combination of any of languages including binary values, arithmetic equations, images, any text with different style and fonts. Messages are the composition of symbols, local cultural languages which preserves white space.

The method of human communication, either spoken or written, consisting of the use of words in a structured and conventional way.

Figure. 1. (a) shows migration issues between original message to the encryption or decryption state. This converts binary data into the ASCII format. Receiver end this should be the reverse process to generate decoded information.

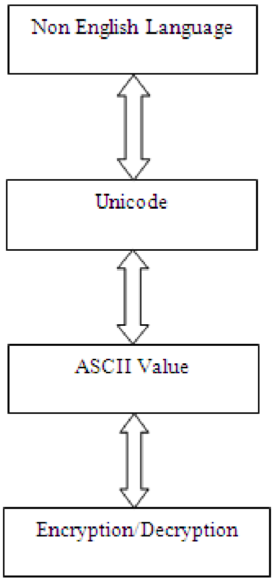


Fig. 1. (a) Transition of non English Language

Unicode: Worldwide encoding/translating standard format with various dialects and scripts, by which each letter, digit, or image (i.e., binary information) is doled out a one of a kind numeric esteem that applies crosswise over various stages and projects. Unicode is an industry standard format for reliable encoding content with the all inclusive coded character set standard; the code involves 128,000 characters covering 135 scripts. The most widely recognized encodings are actualized in numerous current innovations XML, java and other programming builds.

ASCII Value: Character encoding standard speak to content in system, portable correspondence hardware and other systems administration gadgets and they bolster additional usefulness. The encoding incorporates 26 alphabetic characters, 10 numerical digits, 25 realistic images, and control characters.

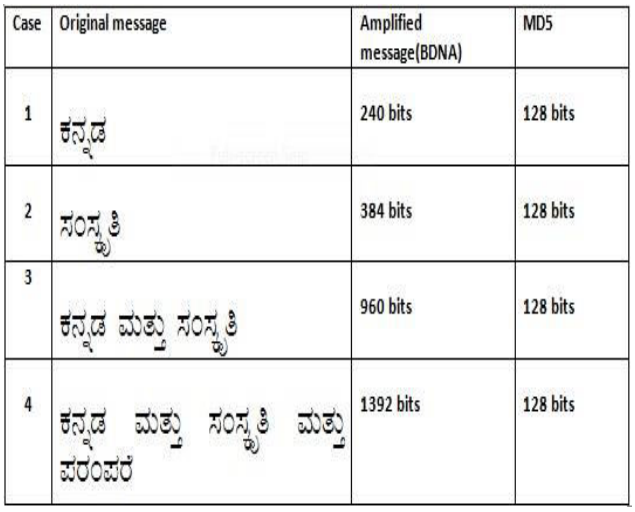
Encryption/Decryption: Encryption changes over unique message into less number of encoded information and secures the secrecy of computerized information. The Decryption changes over encoded information into the first message (intelligible frame).

➢ Comparison

Wireless sensor node is a battery powered consumes more energy for transmitting and receiving huge payload. In the table 1 is a comparison of BDNA and MD5, which gives energy awareness in respective algorithm.

The length of the message digest generated enhances the security of the system. In order to generate longer security message it takes much computational resource and computing time. Since in WSNs the sensors are provided with less computational resources and less battery power, the message digest algorithms should not take over available resources to generate the digest. Thus we need an optimal algorithm that will generate longer digest and that can be generated in less computational time.

Table 1. Comparison of BDNA and MD5



Case	Original message	Amplified message(BDNA)	MD5
1	ಕನ್ನಡ	240 bits	128 bits
2	ಸಂಸ್ಕೃತಿ	384 bits	128 bits
3	ಕನ್ನಡ ಮತ್ತು ಸಂಸ್ಕೃತಿ	960 bits	128 bits
4	ಕನ್ನಡ ಮತ್ತು ಸಂಸ್ಕೃತಿ ಮತ್ತು ಪರಂಪರೆ	1392 bits	128 bits

➢ Performance

The chart deals with delineates vitality utilization regarding BDNA and MD5.

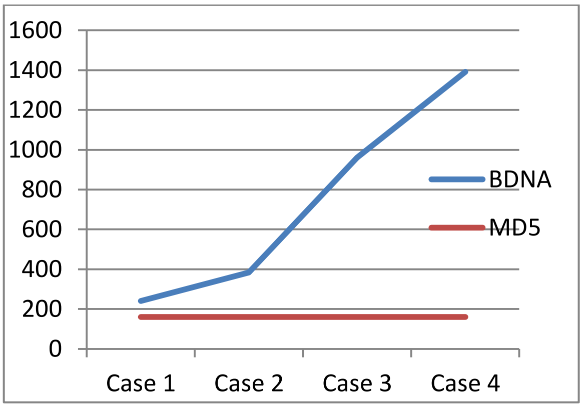


Fig. 2. Comparison between BDNA and MD5

According to the graph we state that BDNA consumes more energy compare to MD5. Message digest broadcast less data with high accuracy and authenticate the data which comes from genuine sender with the highest confidentiality margin.

Case 1: original message consumes 240 bits of Amplified message and 128 bits of md5.
Case 2: original message consumes 384 bits of Amplified message and 128 bits of md5.
Case 3: original message consumes 960 bits of Amplified message and 128 bits of md5.
Case 4: original message consumes 1392 bits of Amplified message and 128 bits of md5.

This proposed system message approval updates security with light weight hash work; to perceive true blue data from intruder's data, warrant techniques are frequently used to check the uprightness of the got data in a correspondence structure. There are a couple of message affirmation plots in remote sensor frameworks. The affirmation techniques were used as a piece of the genuinely constrained remote sensor network circumstances.

This proposed paper gives improved variation of security with a less execution/run time. The more prominent security depends upon the length of MD created by the hash limits which is confined by the degree of commitment to the computation.

IV. CONCLUSION

The proposed system clearly proves that transmission of non English languages needs transition between Unicode, ASCII values finally ends with encryption and decryption. MD5 encrypts huge data and produces 128 bit output. This system enhances the movement over English users to non English user with the enhanced security. This can help reach to the more extensive group of the sensor users. The future work will concentrate on the conceivable assaults and cryptanalysis to measure quality. The result shows that proposed plan gives favored security over the present one.

REFERENCES

[1] 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.

[2] Prajapati Ashishkumar B, Prajapati Barkha, 2016.Implementation of DNA Cryptography in Cloud Computing and Using socket Programming. IEEE, New Delhi, Jan 2016, p. 07-09.

[3] 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.

[4] 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.

[5] 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.

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

[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] 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

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

[10] M. A. Simplicio, et aI., "Comparison of authenticated-encryption schemes in wireless sensor networks," in IEEE LCN 2011, pp. 450- 457.

[11] Y. Shuai, et aI., "A new design of security wireless sensor network using efficient key management scheme," in IEEE NIDC 20 I 0, pp. 504-508.

Authors’ Profiles

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 6 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 4 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 17 years. Life membership in Indian Society for Technical Education (ISTE).