RESEARCH ARTICLE OPEN ACCESS

# Message Authentication in wireless Networks using HMAC algorithm.

Mr. Tadesse Hailu Ayane*****, Mr.Temesgen Bailie Workie**,
Mr.G.Subba Rao,Lecturer***,

***(***Lecturer & Department Head, School of Electrical Engineering & Computing, Adama Science & Technology University)*
*** (Lecturer, School of Electrical Engineering & Computing, Adama Science & Technology University)*
**** (Research Scholar, Sri Satya Sai University, India)*
*Corresponding Auther: Mr. Tadesse Hailu Ayane*

## ABSTRACT

A message is to be transferred from one network to another across some sort of internet. To do this a logical information channel should established by defining a route through the internet from source to destination with the help of some protocols. A security-related transformation on the information to be sent, with some secret information as secret key will be shared by the two networks and, it is hoped, unknown to the opponent. Wireless networks are increasingly being used in the network with limited cost and low equipment requirement. However, the growing popularity and widespread applications of wireless networks are directly proportionate to their security exploitation. The strength of its infrastructure also becomes the point of its greatest availability in the network. Thus decreasing the confidence level of the system as it pertains to availability, reliability, data integrity and privacy concerns. Message authentication is used to protecting the integrity of a message and validating identity of originator. The algorithm used in this paper for authenticating messages is Hash Message Authentication Codes (HMAC) with stream ciphering.

**Key words:** Stream cipher, HMAC algorithm, constrained environment, WEP protocol.

Date of Submission: 18-05-2018 Date of acceptance: 01-06-2018

## I. INTRODUCTION:

In the networks providing Key Authentication for the message is a standard challenge and response mechanism that makes use of WEP. While the message is encrypting the access point is used to generate shared secret key and responsible for providing authentication to the message. The authenticating client will forward the encrypted text to the access point for verification. Authentication succeeds if the access point decrypts the same challenge text and gets the original message. For Implement above operation a compact HMAC by the use of stream ciphering is presented in this paper.

A hash function such as SHA does not relay on a secret key that is why it will not be used in MAC. There are number of protocols which will support secret key into hash algorithm among that the best suit of protocol is HMAC .HMAC is the essential secured algorithm to implement in MAC for internet protocol security.

In the wireless environment Wireless ad hoc networks are the decentralized networks where there is no infrastructure to manage the traffic for the information between the existing nodes. The active nodes status was determined by the routing protocol in the network design. By using the operating environment and purpose of the nodes will find the limitation in the network.

## II. HMAC ALGORITHM:

2.1 HMAC Design Objectives.

- To use, without modifications, available hash functions. In particular, hash functions that perform well in software, and for which code is freely and widely available.
- To allow for easy replace ability of the embedded hash function in case faster or more secure hash functions are found or required.
- To preserve the original performance of the hash function without incurring a significant degradation.
- To use and handle keys in a simple way.
- To have a well understood cryptographic analysis of the strength of the authentication mechanism based on reasonable assumptions about the embedded hash function.

2.2 HMAC Algorithm.

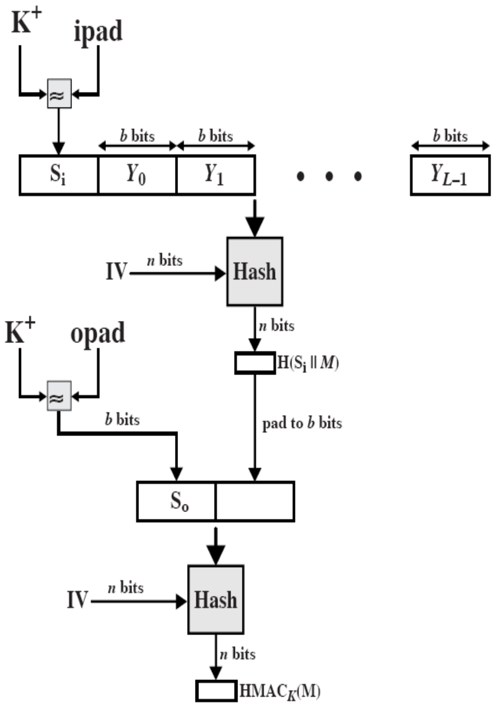


**Fig. 1.** HMAC algorithm representation.

- S-1:append zeros to the left end of k to create a b-bit string k+
- S-2:xor k+ with ipad to produce the b-bit block $S_{i.}$
- S-3:append M to $S_{i.}$
- s-4:apply H to the stream generated in step-3
- S-5:XOR $K^+$ with opad to produce the b-bit block $S_0$ .
- Step-6: Append the hash result from step-4 to $S_O$ .
- Step-7:Apply H to the stream generated in step6 and output the result.
- Ipad : a string of repeated 0x36
  - 00110110,00110110, . . .,00110110
- Opad : is a string of repeated 0x5C
  - 01011100,01011100, . . .,01011100

$$\mathbf{HMAC(K,M) = H(\ (K^+ \oplus opad)\ |\ H(\ (K^+ \oplus\ ipad)|\ M)\ )}$$

2.3 Stream cipher structure.

A typical stream cipher encrypts plaintext one byte at a time, although a stream cipher may be designed to operate on one bit at a time or on units larger than a byte at a time. The output of the generator, called a **key stream**, is combined one byte at a time with the plaintext stream using the bitwise exclusive-OR (XOR) operation. The following parameters are the Design considerations for a stream cipher. The encryption sequence should have a large period. A pseudorandom number generator uses a function that produces a deterministic stream of bits that eventually repeats. The longer the period of repeat the more difficult it will be to do cryptanalysis. This is essentially the same consideration that was discussed with reference to the Viennese cipher, namely that the longer the keyword the more difficult the cryptanalysis.

The key stream should approximate the properties of a true random number stream as close as possible. For example, there should be an approximately equal number of 1s and 0s. If the key stream is treated as a stream of bytes, then all of the 256 possible byte values should appear approximately equally often. The more random-appearing the key stream is, the more Randomized the cipher text is, making cryptanalysis more difficult.

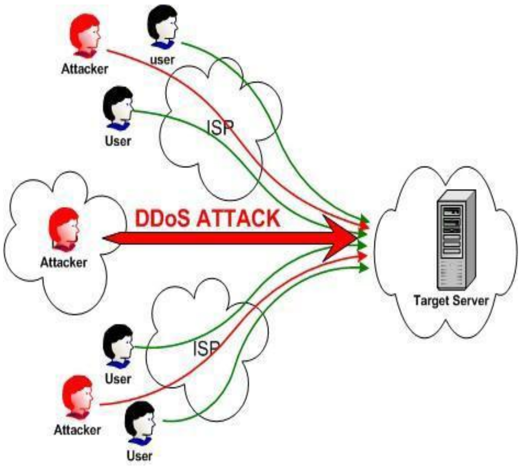
2.4 Wired equivalent privacy protocol .Wired Equivalent Privacy (WEP) Protocol is a standard security feature in the IEEE 802.11 standard, for wireless networks to provide confidentiality and encryption to the network. WEP is unsecured because any one can crack with the help of automated tools. Hence this protocol is will be used only when some encryption standard have to include.

## III. NETWORK AVAILABILITY

3.1 Node Failure and Topological Changes.

When there is more redundancy in the network generally network node is going to be failed. For higher amount of data transmission network it has to adjust the topology. This can be done by using the network routing protocol.

3.2. Denial of Service Attacks. It is the most common attack to deny the network availability. This attack is also named as Physical level attack.



To transmit the data between two nodes in wireless environment we use CSMA/CA (carrier sense multiple access with collision avoidance)protocol. While transmitting data first check the availabily of the channel, if the channel is idle then only data will be passed through the channel otherwise it has to wait until the channel is free.

### 3.3 Passive Attack.

These attacks are affecting the confidentiality of the data. The intruder does not modify the data, only monitors and predicting the data. This attack will happen in the network when there is no encryption for the data.

### 3.4. Active Attack.

These attacks will bring many changes in the network data. It will modify, completely delete the data. Some examples of active attacks are data interruption, interception, modification and fabrication.

## IV. RELATED WORK AND THE STRUCTURE OF THE PAPER.

As indicated, compact MAC implementations is very help full in restricted places. Possible implementations of hash in such environments, based on block ciphers, are surveyed in [11]. On the other hand, stream cipher is always adding with message data. Secure and well-analyzed stream ciphers offered by the stream project are very compact and use limited hardware resources. MAC based stream ciphers are always greater efficiency and minimal resources can be used, about such implementations are explained ind [20], [21], [22], [23]. These approaches concern stream-cipher-based designs dedicated to MAC implementations, combining hashing and encryption within an integrated solution. It is the purpose of this paper to illuminate the use of stream ciphers incompact hashing from a different angle. Here, a one-way block transformation, based on a stream cipher, is first implemented as a stand-alone universal circuit. This can also be turned into an HMAC implementation.

In this paper the data is flowing between two wireless nodes as source-1 to destination-1.The path choosing between these nodes as shown in the results. Result at the time 1.10864 sec assume the source station is 21node and the destination station is at node 27 and the key length .data length are 20 in bits,8 in bytes are shown in the result.

## V. SIMULATION RESULTS:

Test case-1

input.txt

```
1198573890650976858
09776530956043287
6565747589845756809 12
5672875567792094024 93
```

hmac.txt

```
44<;8:6;<3983<:9;8;
3<::9863<893765;:
9898:7:8;<;78:89;3<45
89:5;:889::<53<7357<6
```

output.txt

```
1198573890650976858
09776530956043287
6565747589845756809 12
```

Test case-2

input.txt

```
dhsdyy33 duwu8hef7
f37yr8 hdjeju9hfe3ipd
cnipo73903jkaeklkej
eruoer730903rkle37hkjpdgdfi
gfh72y92bdlwdlk2uepek
```

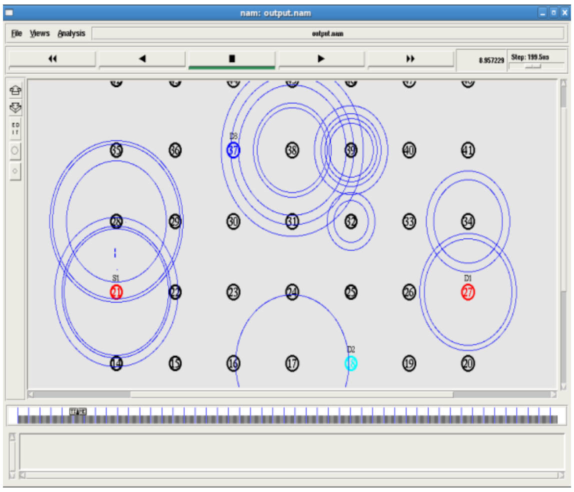
hmac.txt

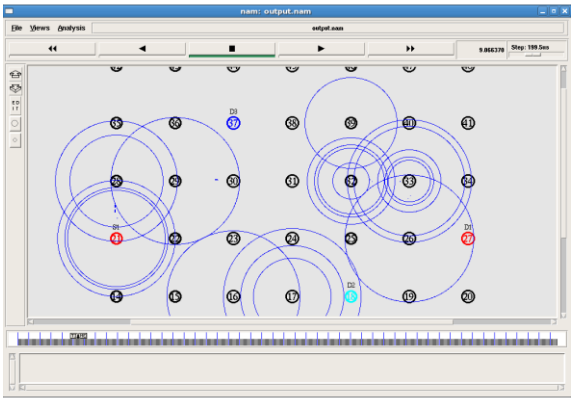
```
gkvg||66#gxzx;khi:
i6:|u;#kgmhmx<kih6lsg
fqlsr:6<36mndhnonhm
huxrhu:63<36unoh6:knmsgjgil
jik:5|<5egozgon5xhshn
```

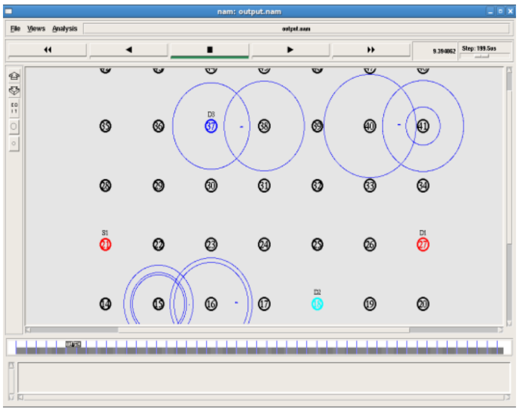
output.txt

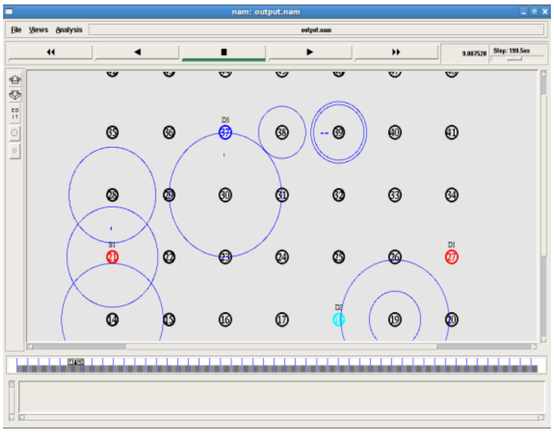
```
dhsdyy33 duwu8hef7
f37yr8 hdjeju9hfe3ipd
cnipo73903jkaeklkej
eruoer730903rkle37hkjpdgdfi
gfh72y92bdlwdlk2uepek
```

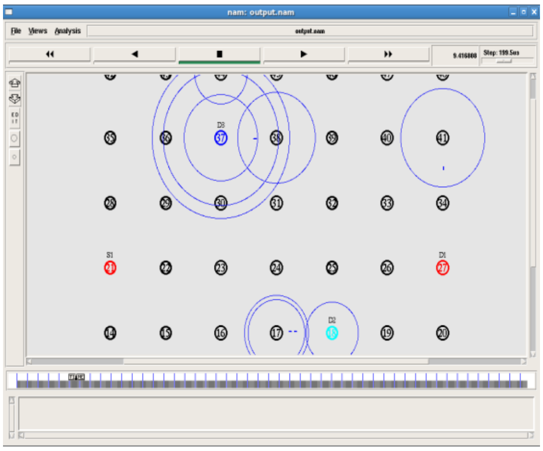
DATA FLOW BETWEEN SOURCE-1TO DESTINATION-1

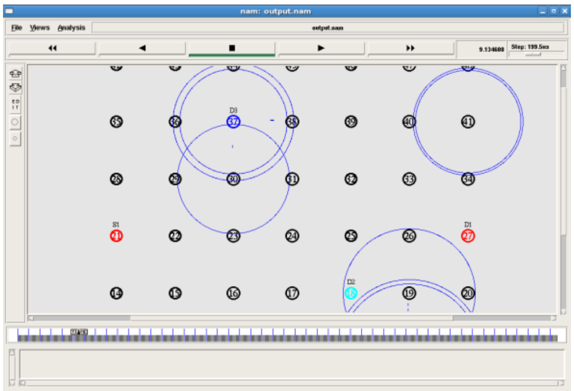


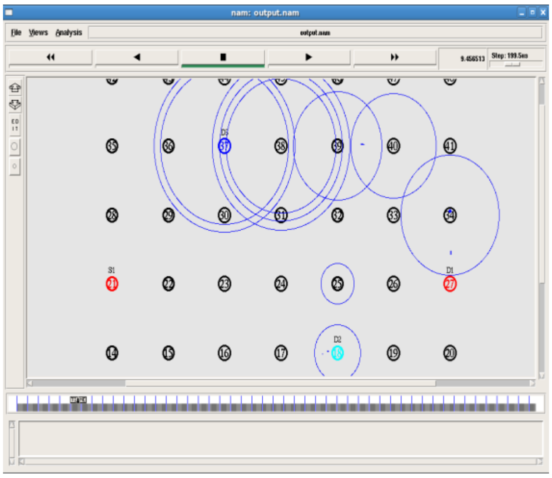


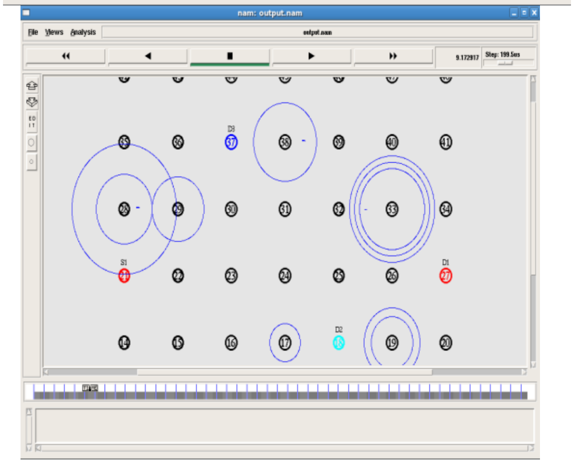












```
============= Result At 1.10864
==============
Source      : 21
Destination  : 27
Token Node   : 22
Key length  : 20 in bits
data length   : 8 in Bytes
Total Routes : 1
============= Result At 1.18320
==============
Source       : 0
Destination  : 18
Token Node   : 1
keylength  : 20 in bits
data length   : 8 in Bytes
Total Routes : 1
=============        Result        At        1.13206
==============
Source       : 12
Destination  : 37
Token Node   : 13
Key length  : 20 in bits
data length   : 8 in Bytes
Total Routes : 1
```

## VI. CONCLUSION:

In the wireless sensor networks for the efficient data transmission with more security can be done by using Hash message authentication algorithm with Stream ciphering was explained in this paper. This research paper develops stream cipher with HMAC and offers more security and efficient data transmission.

## REFERENCES:

[1]. M. Ohkubo, K. Suzuki, and S. Kinoshita, "CryptographicApproach to 'Privacy-Friendly' Tags,"Proc. RFID Privacy Work-shop, Nov. 2003.

[2]. I. Vajda and L. Buttyan, "Lightweight Authentication Protocols forLow-Cost RFID Tags,"Proc. Second Workshop Security Ubiquitous Computing (Ubicomp '03), Oct. 2003.

[3]. G. Avoine and P. Oechslin, "A Scalable and Provably Secure Hash-Based RFID Protocol,"Proc. Second IEEE Int'l Workshop Pervasive Computing and Comm. Security (PerSec '05), pp. 110-114, 2005.

[4]. K. Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment," Proc. Int'l Conf. Security in Pervasive Computing(SPC '05), Apr. 2005.

[5]. M. Feldhofer and C. Rechberge, "A Case against Currently Used Hash Functions in RFID Protocols,"RFID Security Workshop (RFIDSec '06), printed handout, July 2006.

[6]. A. Bogdanov, G. Leander, C. Paar, A. Poschmann, M. Robshaw, and Y. Seurin, "Hash Functions and RFID Tags: Mind the Gap,"Proc. Workshop Cryptographic Hardware and Embedded Systems (CHES '08), 2008.

[7]. S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo, "Security Analysis of a Cryptographically Enabled RFID Device," Proc. USENIX Security Symp., pp. 1-16, 2005.

[8]. ECRYPT, "The Estream Project,"The eSTREAM Portfolio,revi-sion 1, Sept. 2008.

[9]. H. Krawczyk, "LFSR-Based Hashing and Authentication,"Proc.Ann. Int'l Cryptology Conf. (CRYPTO 94), pp. 129-139, 1994.

[10]. B. Zoltak, "VMPC-MAC: A Stream Cipher Based Authenticated Encryption Scheme," Cryptology ePrint Archive, Report 2004/301, 2004.

[11]. D. Whiting, B. Schneier, S. Lucks, and F. Muller, "Phelix—Fast Encryption and Authentication in a Single Cryptographic Primi-tive," Ecrypt Stream Cipher Project, Report 2005/020, 2005.

[12]. K. Wirt, "ASC a Stream Cipher with Built in MAC Functionality," Int'l J. Computer Science, vol. 2, pp. 131-136, 2007.

[13]. P. Hawkes, M. Paddon, and G.G. Rose, "The Mundja Streaming MAC," Cryptology ePrint Archive, Report 2004/271, 2004.

[14]. J. Kaps, K. Yuksel, and B. Sunar, "Energy Scalable Universal Hashing," IEEE Trans. Computers, vol. 54, pp. 1484-1495, 2005.

[15]. M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," Proc. Ann. Int'l Cryptology Conf. (CRYPTO '96), pp. 1-15, 1996.

[16]. H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," IETF RFC 2104, 1997.

[17]. ANS Institution, "Keyed Hash Message Authentication Code," ANSI X9.71, 2000.

[18]. National Institute of Standards and Technology, "The Keyed-Hash Message Authentication Code (HMAC)," FIPS PUB 198,Information Technology Laboratory, 2002.

[19]. J. Kim, A. Biryukov, B. Preneel, and S. Hong, "On the Security of HMAC and NMAC Based on HAVALl, MD4, MD5, SHA-0 and SHA-1," Proc. Conf. Security and Cryptography for Networks (SCN '06), pp. 242-256, 2006.

[20]. National Institute of Standards and Technology, "Secure Hash Standard," FIPS PUB 180-1, Information Technology Laboratory,1995.

[21]. GAO, "GAO-05-551 Radio Frequency Identification Technology," www.gao.gov/new.items/d05551.pdf, May 2005.

[22]. European Commission, "Draft Recommendation on RFID Privacyand

[23]. Security,"http://www.edri.org/edrigram/number6.4/ec-recommandation-rfid, Feb. 2008.

[24]. G. Avoine, "RFID Security & Privacy Lounge," www.avoine.net/ rfid/, 2009.

[25]. P. Siekerman and M. van der Schee, "Security Evaluation of the Disposable OV-chipkaart v1.7," System and Network Eng. Dept.,Univ. of Amsterdam, Apr. 2008.

[26]. J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, "UMAC: Fast and Secure Message Authentication," Proc. Ann.Int'l Cryptology Conf. (CRYPTO '99), pp. 216-233, 1999.

[27]. B.Schneier,"'SchneieronSecurity'—SHA-1HasBeen Broken,"http://www.schneier.com/blog/archives/2005/02/,200

Mr. Tadesse Hailu Ayane "Message Authentication in wireless Networks using HMAC algorithm. "International Journal of Engineering Research and Applications (IJERA) , vol. 8, no.5, 2018, pp.51-56