International Journal of Advanced Research in Engineering Technology & Science
ISSN: 2394-2819
Email: editor@ijarets.or Volume-4, Issue-7 July- 2017 www.ijarets.org

IMPLEMENTATION OF NODE AUTHENTICATION FOR WSN USING HASH CHAINS

SHASHANK TRIPATHI, GAURAV AGGARWAL
GRD Institute of Management & Technology
Dehradun, Uttarakhand

ABSTRACT— This paper presents the design and implementation of a lightweight node authentication protocol which comprises of node registration, node authentication and key establishment phases. The solution leverages the low computational overheads associated cryptographically secure one-way hash chains and Elliptical Curve Cryptography (ECC) without using any digital signature algorithm or any public key cryptography. The usage of hidden generator point derived from hash-chains provides defense against a man-in-the-middle attack which is prominent in ECDH (Elliptical Curve Diffi e-Hellman) due to lack of entity authentication. The authentication protocol has been simulated on Tossim and its performance bench marking has also been carried out.

INTRODUCTION

This section gives wireless sensor network of Things and its enabling technologies. It also discusses the basic overview of WSN security features, security architecture, and security challenges in WSN. Wireless sensor network is a correspondence framework between hubs. It has been set up either straightforwardly or by implication by furnishing help with different hubs, in light of the fact that in remote sensor organize every hub may go about as a switch or a basic hub. Remote system are made out of numerous self-governing hubs that convey to each other with no framework. Since the topology of the system is alterable in this way any hub can without much of a stretch join or leave whenever. Remote sensor organize has a possess design and element topology. Remote systems administration is a strategy by which homes, broadcast communications systems and venture establishment stay away from the costly procedure of bringing links into a building, or as an association between different gear areas. Remote broadcast communications systems are normally actualized and regulated utilizing radio correspondence. The insurance of data [1] [2] for long stretch time is extremely basic in numerous conditions. Power is the most vital sympathy toward convey between wireless nodes.

In mid 1970s, the Mobile Ad hoc Network (MANET) was called as bundle radio system, which was supported by Defense Advanced Research Projects Agency (DARPA). They had a venture named parcel radio which has a few remote terminals that could speak with each other on combat zones. It is interested to note that these early parcel radio frameworks foresee the Internet and to make sure were the piece of the motivation is unique to Internet Protocol suite. The whole life cycle of Ad hoc systems could be portrayed into the principal, second and the third era Ad hoc organizes frameworks. Display day Ad hoc arranges frameworks are measured the third era. The original backpedals to 1972. Around then, they were called as PRNET (Packet Radio Networks). In concurrence with ALOHA (Arial Locations of Hazardous Atmospheres) and CSMA (Carrier Sense Medium Access), approaches for medium get to control and a sort of separation vector steering PRNET were utilized on a trial premise to give diverse systems administration capacities in a battle situation.

The second era of remote systems rose in 1980s, when the Ad hoc organize frameworks were further upgraded and actualized as a piece of the SURAN (Survivable Adaptive Radio Networks) program. This giving a bundle changed system to the portable battleground in an environment without framework. This program turned out to be valuable in enhancing the radios' execution by making them littler, less expensive, and strong to electronic assaults.

OBJECTIVE

- Literature Survey
- Implementation of a lightweight node authentication protocol
- Registration of nodes
- Authenticate nodes
- Establishment of key

LITERATURE REVIEW

In this section of paper the literature review is presented which includes several research area is being offered.A wireless network is any kind of computers network that uses wireless data connections for relating network nodes. Wireless network are composed of many autonomous nodes that communicate to each other without any infrastructure. Wireless network uses wireless data connections to connect the network nodes. Wireless communication does not require any wired infrastructure to transfer data among the users. Using electromagnetic waves, mobile users transmit and receive data over the air. Wireless communication is much more popular due to its simplicity, mobility and cost retaining installation.

This section gives a detailed description of establishment node in WSN.

Sensor networks have different requirements than other wireless networks. The need for robustness and scalability leads to the design of localized algorithms, where sensors only interact with other sensors are stricted vicinity and have at best an indirect global view.

Authentication mechanisms using Hash Chains are considered to be computationally feasible for resource constraint network like WSN. Hash Chains were fi rst proposed by Lamport who used it for generating one-time password11. This involves applying a hash function h(.) repeatedly z times to a seed s to form a hash chain of length z. The hash (.) is easy to compute but hard to invert e.g., h(h(h(s))) gives a hash chain of length 3 and can be denoted by h3 (s). The initial element of the hash chain is called the seed and the last element is called committed value or the tip of the hash chain. The tip of the chain is public and is distributed among the nodes and the elements of the chain are consumed one after other until the secret key is free. Hash chains find exclusive use in data integrity and entity authentication. The i th element of the hash chain denoted as Ki is expressed as:

$$Ki\ (s) = h(h\ z- i\ (s)) \quad \ldots\ldots(1)$$

The committed value of the chain is made public while as the seed acts as private or secret value. The scheme does not overcome the need for an authenticated initial key-exchange. By the defi nition of entity authentication, Lamport's one-time passwords do not provide entity authentication as there is no proof of an active communication between the two parties. Some of the relevant schemes offering entity authentication as part of overall access control have been given by Zhou12 et al. which is based on ECC and ECC-based digital signature scheme ECDSA. It has been proved to be an energy effi cient than RSA. It achieves node authentication and key establishment for new nodes by including both node identity and node bootstrapping time into the authentication procedure. However, it uses timestamps and assumes that each sensor node can

sustain time interval before it can be compromised. Therefore, for practical implementations, it is not thought to be convenient. Huang proposed NACP13 scheme which is based on Hash chains and ECC. It is simple, energy effi cient supports new node addition but has been found to be vulnerable to replay attack and new node masquerading attacks. This is attributed to the absence of any mutual authentication between node and base station. It also lacks hash chain renewability. Other schemes supporting authentication where given under ENACP an enhancement over NACP, PACP and NDACP14. Out of the schemes discussed only ENACP provides authenticated broadcast.

APPROACH

The authors argue in favor of designing localized algorithms and present directed diffusion as a set of abstractions that describe the communication patterns underlying such algorithms. The design features differ from traditional wireless networks and are data-centric and application-specific. Data-centric refers to the fact that in sensor networks we are mostly interested in retrieving information matching certain attribute values and very rarely we will be interested only in data from a specific node. This approach decouples data from the sensor that produced it and unique identification of nodes is of secondary importance. Application-specific refers to the awareness across all layers of the specific application so that intermediate nodes can perform data aggregation, caching and informed forwarding. The authors proceed to describe a two-level cluster formation algorithm, where cluster heads are elected based on available energy. They present a localized algorithm for object tracking to demonstrate the difficulties that arise. The design is difficult because localized algorithms need to produce a certain global behavior with at best indirect global knowledge. Furthermore, localized algorithms tend to be sensitive in the choice of parameter values.

METHODOLOGY AND IMPLEMENTATION

The proposed scheme presents a comprehensive pair-wise entity authentication protocol with the proper key establishment in 4 phases i.e. Initialization, Node registration, Key generation and Node authentication and Node to Node authentication involving Node identities. We propose a unique method for Node Authentication where there would be no key transmitted over the network to establish a connection with the device. The connection would be established using an encrypted image. For encryption of image data, Chaos-based image encryption algorithm is used. In Chaos-based image encryption shuffling the positions and changing the pixel values of the image pixels are combined to confuse the relationship between the cipher image and the plain-image. The proposed image encryption algorithm has three major steps. Firstly, the Arnold cat map is used to shuffle the positions of the image pixels in the spatial-domain. Secondly, applying 128 bit key on the image. Thirdly, EXOR-ing the generated sequence with data stream. Existing Krishnamurthy et al. method is using three 1D chaotic maps, whereas we are using a single 2D chaotic map. We are using 128 bit key for encryption whereas Krishnamurthy et al. implemented 120 bit key for encryption. Algorithm used for encryption using Arnold's 2D cat map.

The connection establishment phase has 4 steps as follows:

Step1: The initiator send request to the responder using the encrypted image (Ek).

Step2: The responder receives the request and decrypts the image using decryption algorithm. If the received image matches with the decrypted image then it send signature to initiator for verification.

Step3: The initiator compares the received signature with stored signature. If it matches it sends an acknowledgement (Ack) to the responder.

Step 4: Responder verifies the acknowledgement and the connection is established.
Here: Initiator is our base station and responder is the node.

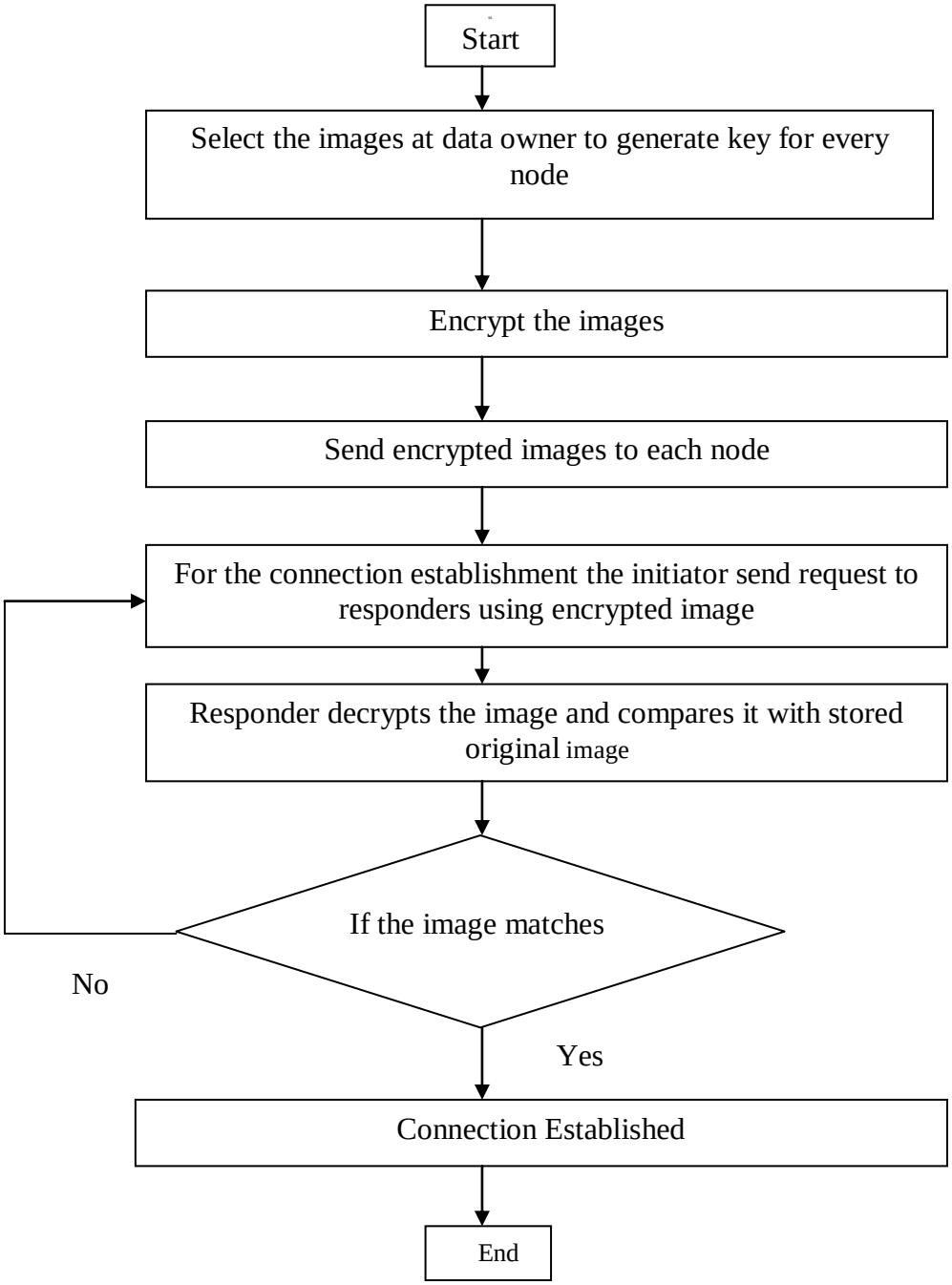


Figure: Proposed System Flow Char

RESULT AND ANALYSIS

Qualitative Result Analysis

For qualitative result, the proposed approach is tested on few parameters are used for this: Security, utilization, time interval, traffic overhead.

For performance comparison, the result of proposed work is compared with existing work. The results explain that the proposed work helps in increasing the prevention of denial of sleep attack and security of the network. Therefore the proposed work has higher security with low overhead and. The comparison of existing and proposed work on the basis of above parameters is depicted

Algorithm for encryption using Baker's Map

Step1. I ← read image
Step2. MD5 ← hash map of I /* authenticate image */
Step3. SHA-1 ← hash map of I
Step4. while no not equal to 1
Step5. x ← two random numbers between 1 and 100
Step6. alpha ← 1.9999
Step7. beta ← 0.25
Step8. nStop ← 400 /* number of iterations */
Step9. for n = 1:nStop
. s ← sign of x(1) /* calculate signum*/
fx(1) ← alpha*x(1) - s
fx(2) ← beta*x(2) + s/2.0
end for
Step10. R ← mean of fx
Step11. Ss ← inverse of R
Step12. No ← ss*R
Step13. end while
Step14. x_uid ← random 9 numbers
Step15. C ← R^e X x_uid
Step16. SPRK ← x_uid X UID^d
Step17. R_s1 ← UID^{r_s1} X $x\_uid^{2*r\_s1}$
Step18. **Encrypt image using value of R**
for i ←1 to r /* rows */
for j ← 1 to c /* columns */
. for k ←1 to n /* channels */
Eimage[i,j,k] ← I(i,j,k) X R_s1
end for k
end for j
end for i
Step19. Display encrypted image
Step20. **Decrytp image**
for i ←1 to r /* rows */
for j ← 1 to c /* columns */
. for k ←1 to n /* channels */
Dimage[i,j,k] ← Eimage(i,j,k) / R_s1
end for k

end for j
end for i
Step21. Ih ← calculate hass code MD5 of Decrypted image
Step22. DIh ← calculate hash code SHA-1 of Decrypted image
Step23. if MD5 is equal to Ih then
if SHA-1 is equal to DIh then
Display Hash matches
else
Display No match
end if
else
Display No match
end if
Step24. results ← calculate NPCR and UACI on Original and Decrypted image

RESULTS

Output Received after running the Code of {proposed RSA Baker Map.
Ouput:
Product =143

Explanation:
For RSA two prime numbers are generated and their product is calculated.

Output:
*** Generated Public key is (59,143)***
*** Generated Private key is (59,143) ***

Explanation:
Public key and Private keys are generated using the products through RSA algorithm.

Output:
*** Message: Hello
Explanation:
Hello message is transmitted over the net.

Output:
Hash Map MD5
5212633240a929a79bb327acfbfc45ca

Explanation:
Hash Map - MD5 is generated for the data transmitted over the network.

Ouput:
Hash Code SH1
d8c86693ed0c213beb5fef9470f6b4afa8bfd9b4

Explanation:

Hash Map – SH1 is generated for the data transmitted over the network.

Output:
Message in ASCII form
72 101 108 108 111

**** Encrypted message is ***

118 114 32 32 105

72 101 108 108 111

Explanation:
Transmitted data, here Hello, is fisrt converted into ASCII form and then encrypted before transmitting it over the network.

Output:
*** Decrypted message is: ***
Hello

Hash Code MD5 Transmitted data
5212633240a929a79bb327acfbfc45ca

Hash Code SH1
d8c86693ed0c213beb5fef9470f6b4afa8bfd9b4

Explanation:
The transmitted message is decrypted and Hash codes are again calculated.

Output for signature:
Value generated 38

Value generated 11

R = 11

R X inv(R) = 11

Signatures of Encrypted = zyzwzwwswuxwrwzkzwrkwmxkuenwcks[

Explanation:
Two values are generated for signature. Lesser value is considered as R value and multiplied with it's inverse. Signature is then encrypted and transmitted over the network.

Output (Signature):
Decrypted = zyzwzwwswuxwrwzkzwrkwmxkuenwcks[

Explanation:
Signature is decrypted at the receiver's end.

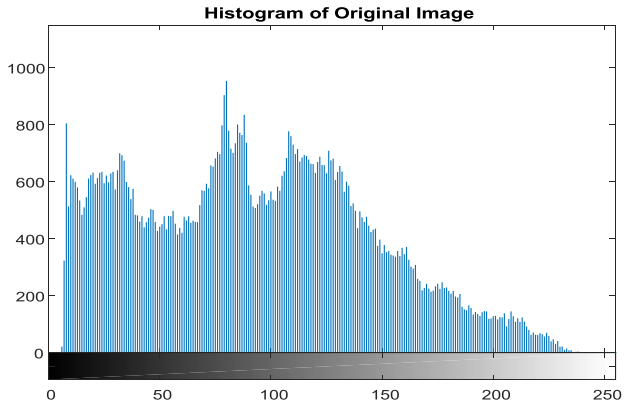
Output:
Messages match
Hash code MD5 Received Data
5212633240a929a79bb327acfbfc45ca

Hash Code SH1
d8c86693ed0c213beb5fef9470f6b4afa8bfd9b4
Hash codes match

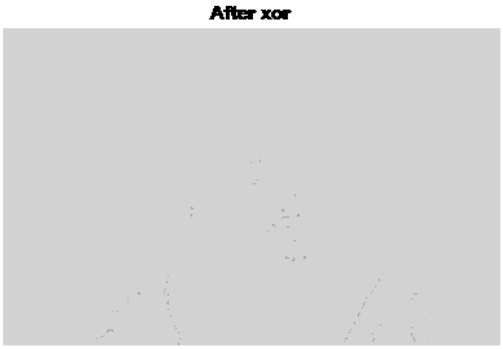
Signatures match.

Explanation:
Messages, Hash codes and Signatures are matched, if they match transmission is successful.

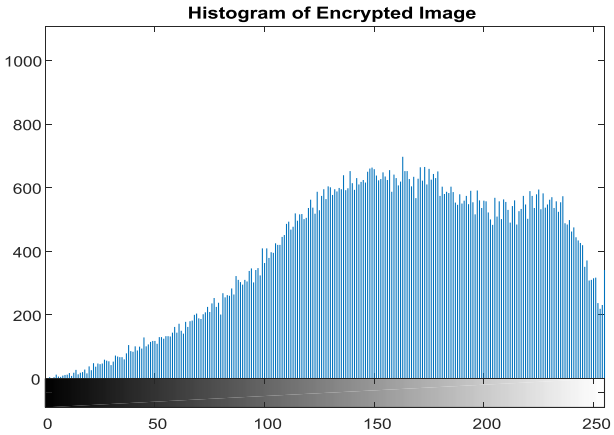
Original image loaded for transmission.



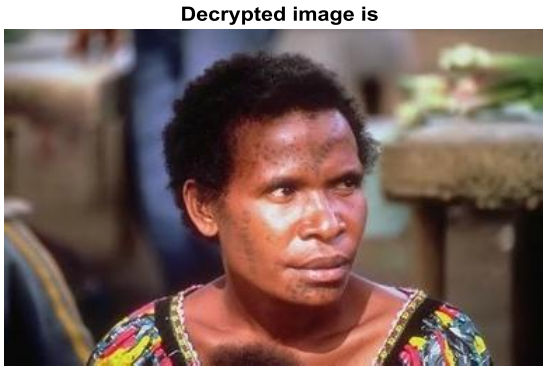
Histogram of the original image read.



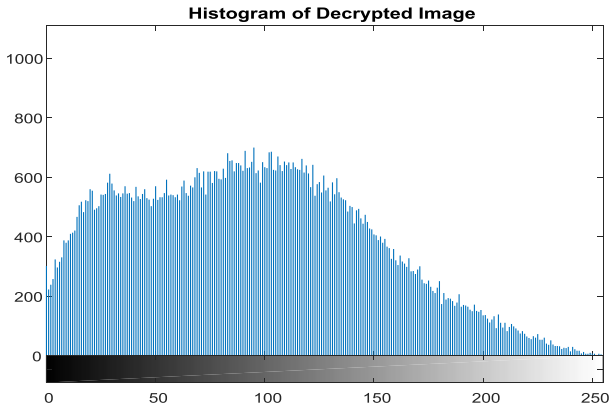
Encrypted image transmitted over the network.



Histogram of Encrypted image



Shows image decrypted at receiver's end.



Histogram of Decrypted image.

Output: Hash Codes generated before image is transmitted. Image is broken into four equal parts before it is transmitted over the network.

Results obtained when image is passed
Hash Map MD5 I part
cb6fb5a6ed75f6370365dd9e8ada4d9c

Hash Map SHA-1 II part
463940ee267a596f3fff68b68471d183317af319

Hash Map SHA-256 III part
92d6e988110f2a10f2e3224b3254995762c6fb694143c1008dae7b4daea4ad39

Hash Map SHA-512 IV part
92d5226330138fc4075479dbfd86e9b197a9c7a7e11ca01361f2e83f960916667ce54f109697cca62ee82ca8c2c
4908ab4090262b6d92de1c388dc0def432713

Output: Hash codes of the received images at the receiver's end.
Hash Map MD5 I part
cb6fb5a6ed75f6370365dd9e8ada4d9c

Hash Map SHA-1 II part
463940ee267a596f3fff68b68471d183317af319

Hash Map SHA-256 III part
92d6e988110f2a10f2e3224b3254995762c6fb694143c1008dae7b4daea4ad39

Hash Map SHA-512 IV part
92d5226330138fc4075479dbfd86e9b197a9c7a7e11ca01361f2e83f960916667ce54f109697cca62ee82ca8c2c
4908ab4090262b6d92de1c388dc0def432713

CONCLUSION AND FUTURE SCOPE

The proposed entity authentication scheme was implemented by leveraging computationally light Hash chains and Elliptical Curve Cryptography. Shared pairwise key have been derived by using Hidden

Generator Points and is tied to the Node identities and hash chain values. This gives a safeguard against MIM attack eminent in ECDH. The Framework doesn't use any digital signature mechanism to achieve authenticated broadcasts. Instead, secret value of hash chains has been used for the purpose. The framework can be embedded into any WSN based application where Entity authentication is a requirement.

REFERENCES

1. I.F.Akyildiz,*etal*.,A Survey on Sensor Networks,*IEEE Communications Magazine*,pp.102–114,(2002). Adrian Perrig.
2. John Stankovic and David Wagner, Security in Wireless Sensor Networks, *Communication soft e ACM*,vol.47,no.6, pp.53–57,June(2004).
3. Adrian Perrig, Robert Szewczykand J.D.Tygar, Victor Wenand David E.Culler, SPINS: Security Protocol for Sensor Networks,*Proceedings of 7th International Conferenceon Mobile Networking and Computing*,vol.8,no.5,pp.189–199,(2001).
4. D.Hankerson,*etal*.,Guide to Elliptic Curve Cryptography, Springer,(2004).
5. Bernard Menzes, Network Security and Cryptography, Cengage Learning.
6. N.Gura, A.Patel,A. Wander, H.Eberleand S.C.Shantz, Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs. CHES2004,vol.3156of LNCS,(2004).B.Arazi, Certifi cationo fdl/ec Keys, *Proceeding softhe IEEE*,P1363.
7. Ravi Kishore Kodali, *et al.*, Implementation of ECC with Hidden Generator Point in Wireless Sensor Network, *IEEE 2014*,978-1-4799-3635-9/14,(2014).
8. A.H.Moonand Khan Ummer ,Authentication Protocols for WSN using ECC and Hidden Generator ,*International Journal of Computer Applications*,(0975–8887)vol.133,no.13,(2016).
9. TinyOS.http://www.tinyos.net