Journal of Computer Science 9 (11): 1556-1565, 2013
ISSN: 1549-3636

doi:10.3844/jcssp.2013.1556.1565 Published Online 9 (11) 2013 (http://www.thescipub.com/jcs.toc)

A NOVEL APPROACH FOR INFORMATION SECURITY IN AD HOC NETWORKS THROUGH SECURE KEY MANAGEMENT

[1]Suma Christal Mary, S., [2]M. PallikondaRajasekaran and [3]Y. ChrisbinJeeva

[1]Department of Computer Science and Engineering, Kalasalingam University, Krishnankoil, India
[2]Department of ICE, Kalasalingam University, Anand Nagar, Krishnankoil, India
[3]Department of MCA, PSN College of Engg and Technology, Palayamkottai, India

Received 2013-05-21, Revised 2013-06-26; Accepted 2013-10-02

ABSTRACT

Ad hoc networks provide flexible and adaptive networks with no fixed infrastructure and dynamic topology. Owe to the vulnerability nature of ad hoc network, there are lots of security threats that diminish the development of ad hoc networks. Therefore, to provide security for information of users and to preserve their privacy, it becomes mandatory to use cryptographic techniques to set up secure mobile ad hoc network. Earlier cryptographic method based on computational complexity ruins with the advent of fast computing computers. In this proposal, we proposed Secure Key Management (SKM) framework. We make use of McEliece algorithm embedded with Dispense Key designed for key generation and for the key distribution and it is highly scalable with respect to memory. The experimental result shows that our framework provides a high-performance platform to execute key generation, key distribution scenarios. SKM framework reduces execution time of encryption and decryption by minimizing the number of keys.

Keywords: Security, Key Generation, Key Distribution, Ad Hoc Networks, Public Key Cryptography

1. INTRODUCTION

A new archetype for wireless communication is ad hoc network for mobile nodes having no fixed base station or mobile switching centers. Mobile nodes communicate directly with its nodes that fall within the radio rages of each other. Direct communication is always impossible in ad hoc networks, i.e., communication among nodes that do not fall under the radio range of each other. In such a case, nodes proceeds multihop fashion for communication. Mobility nature of the mobile host leads to frequent changes in network topology. Wireless link causes, ad hoc network susceptible to various attacks such as passive, message replay, active impersonation, eavesdropping and message distortion. Authentication, confidentiality and integrity are the most major issues in ad hoc networks.

To overcome the security threats, there is a need for security mechanism that should scales well with the hundreds and thousands of nodes. The primitive solution to this defect is the cryptography, which reinforces on data security, providing the fundamentals for trusted e-commerce and secure communications. Most of the cryptographic techniques depend on the encryption algorithm and key used to generate chiper text from plain text during encryption and vice versa for decryption. The security of an information and encryption algorithm depends on the length of key size. It is recommended to use long keys, which is required to defend against brute force attack. Various cryptographic techniques are proposed. Former method uses symmetric key encryption that depends on single key for encryption and decryption; some of the examples of symmetric key cryptography are DES, 3DES.

Corresponding Author: Suma Christal Mary, S., Department of Computer Science and Engineering, Kalasalingam University, Krishnankoil, India

Symmetric cryptography method requires distribution of keys in prior to communication. Key distribution center is used to distribute key, which is a tedious work. In addition to that it needs to keep the key secretly. These inefficiencies of symmetric encryption method does not suit ad hoc network. Since, they change their topology frequently or hard to find the location of a node or link failure. To distribute key to nodes of a network where there is no prior knowledge on network topology can make use of key pre-distribution method. Key pre-distribution depends on trusted third party rendering them not applicable to ad hoc network. This is due to the lack of trusted infrastructure in ad hoc networks. Also, sharing context prior to network operation begins is not always be practical. Dependence on trusted third party can be eliminated by Distributed Key Pre-distribution Scheme (DKPS). It does not require more information that is based on the underlying network. Therefore, DKPS approach is robust against frequent changing topology and in broken links. Thus, it helps in widespread of secure ad hoc network. It preferably provides secrecy to an entity along with message authentication. Arrival of new nodes, rather than revolution of old nodes must not be allowed by the shared scheme. Integrity, authentication and privacy are the most security requirements that are addressed by building upon a solid key management framework.

Asymmetric cryptography also known as public key encryption overcomes the problem of the key distribution present in symmetric key. It makes use of a pair of key (public and private), one for encryption and another one for decryption. Both keys are mathematically related to each other. Furthermore, it is computationally infeasible to determine the private key, by knowing public key, encryption and decryption algorithm and chiper text. RSA, ElGamal, Elliptic Curve Cryptography are few examples of asymmetric encryption. However, it requires Certification Authority (CA) for generation of key and distribute to user nodes. This necessity is not applicable for ad hoc network for the reasons below. (1) It may be compromised by attackers. (2) CA may become a vulnerable point if the network is not distributed. (3) CA must be available always to carry out key management operations. Because of node mobility availability of CA forever is impossible. Another added problem with asymmetric cryptography is that it requires nodes of ad hoc network to calculate complicated computation. The nodes with less energy may face trouble to carry out this complicated mathematical function. Energy of nodes should also be considered while integrating security objects with the ad hoc network.

Certification based methods are also not applicable for ad hoc network. Since, Exchange of the certificate deals with noticeable expense in resource limited environments. Thus, it leads to a self-sustained key management scheme through a mobile node to take authentication information. This concept depends on the mobile device ensuring secure communication with the server before they are disposed to the action. Self-sustained public key management scheme consists of all involved cryptographic keys in individual nodes before they are aligned. As a consequence there is no communication overhead for authentication for the nodes with other entity ID's.

In our approach, the key distribution function for the secure key distribution is applied based on the Dispense Key approach where the number of keys generated is reduced hugely. SKM prerequisite the primitives for security along with secure information. Low computational complexity in addition to the high degree of security is provided by the security protocol. As the nodes with minimum energy can be turned off or stolen by intruders are limited with physical security. This simulates other nodes to find the key of stolen/turned off node, which causes bottleneck situation as many nodes keep on trying to find the key of a node that went out of communication range because of above reason for recreating the key.

The rest of the paper is structured as follows: Section 2 provides a background on essential terms needed to know before implementing the proposed approach and reviews of related works. Section 3 presents our proposed system. Section 4 experimentally evaluates our approach and its variants. Finally section 5 concludes the paper.

1.1. Related Work

An effectual way of shielding perceptive information while storing on media or transmitted through communicational links is termed as cryptography. There are several methods and techniques are available in Cryptography.

A substitution cipher is one of the methods in which letters are replaced by other letters; on knowing the order of the cipher alphabet someone can decipher the alphabets used. A Letter-Substitution Ciphers is described in (Corlett and Penn, 2010). This approach suffers from the problem of absolute synchronization between sender and receiver additionally the numbers of keys are restricted.

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography, pair of keys

namely public and private keys along with the desired cryptographic operation was generally exits among each user or device that involved in secure communication. Rivest *et al*. (1978) a brief preface is specified regarding the Elliptic Curve Cryptography (ECC), its implementation procedure on Considering the Digital Signature (ECDSA) and key agreement (ECDH) algorithms. Moreover, a small discussion is made concerning the implementation of ECC on two restricted fields such as prime field and binary field. A synopsis of ECC implementation on different coordinated systems called the projective coordinate systems is being endowed. In this approach, the calculation of discrete logarithms is a quite typical one to put into operation.

An outlook of various cryptographic applications which are derived from the proposal of McEliece for the sake of using the error correcting codes for cryptographic purposes are offered by Engelbert *et al*. (2006) and Bernstein *et al*. (2008a) has put forward new-fangled parameters for the McEliece and niederreitercryp to systems thus greatly attaining standard levels of security against all known attacks. These improved attacks are taken as values for new parameters along with the current introduction of list decoding for binary Goppa codes; and the possibility of choosing code lengths that are not a power of 2. Thus resultantly the public-key sizes are significantly much smaller than the previous parameter supplemented for the security purpose. It added a new advantage for McElice, which is included implicitly in our proposed approach.

An ancient public-key cryptosystems even more designed is the McEliece cryptosystem. Based on linear error-correcting codes it is the first always public key cryptosystem developed. This system gains an added advantage because of having very fast encryption and decryption functions. The chief thing to be highly concentrated is that it requires a extremely large public key which makes it highly complicated to use in many real time circumstances. The most probable situation is to advantageously use quasi-cyclic codes since it is characterized to be rich in the compact. Finally, (Berger *et al*., 2009) affords a novel technique to reduce the Key Length in McEliece Cryptosystem. Encryption is carried on representing it as a number M and raising M to a publicly specified power e, then enchanting the remainder while the result is alienated by the widely specified product n, of two large secret prime numbers p and q. The Decryption process is very similar; the only difference is a secret power d is used. All those public key cryptosystem rely on computational complexity of different mathematical problems.

There are many security aspects concatenated with wireless ad hoc networks. Some of them are as follows. As per in (Chan *et al*., 2003; Du *et al*., 2003; Liu and Ning, 2003; Delgosha and Fekri, 2006; Traynor *et al*., 2006; Bernstein *et al*., 2008b; Zhou and Haas, 1999; Kobara and Imai, 2001; Balasubramanian *et al*., 2008) wireless sensor networks use symmetric key techniques for secure communication. The main advantage of symmetric key techniques is its energy efficiency and computational. In symmetric key techniques, secret keys are pre-distributed among nodes before their deployment. To use small memory size to establish secure communication among a large number of nodes and achieve good resilience is the biggest challenge of the key distribution scheme.

However, with a centralized server, security service for critical applications may suffer from low availability and poor scalability due to the base reliability and poor connectivity of ad hoc networks. Furthermore, a single-point failure of centralized server can immobilize the whole network that makes the network extremely defenseless to compromises and denial-of-service attacks. In order to improve flexibility to break-ins in wireless ad hoc networks, Zhou and Haas (1999) has offered the certificate-based approaches to ad hoc networks and present a distributed public-key management scheme for ad hoc networks (Camtepe and Yener, 2004), where multiple distributed certificate authorities are used.

Due to the lack of support for authentication and confidentiality (Du *et al*., 2003), it is unsuitable in critical applications over wireless ad hoc networks. Pairwise key distribution schemes (Liu and Ning, 2003; Delgosha and Fekri, 2006; Traynor *et al*., 2006) are able to bolster authentication. But applying distribution keys leads to produce a large number of keys, which are a major challenge.

1.2. Background

Cryptographic algorithms are classified as follows based on the number of keys used.

1.3. Symmetric Cryptography

Single key is used for encryption and decryption. Sender uses the key for encryption of plaintext and converts it to the ciphertext. Receiver uses the same key to decrypt the Ciphertext into plaintext. Having knowledge of algorithm and pieces of ciphertext is not sufficient to steal the plaintext. If the key is known to an unauthorized person, then he may retrieve the documents easily. Therefore, secrecy depends on the key. Information is secured as long as the key is kept secret.

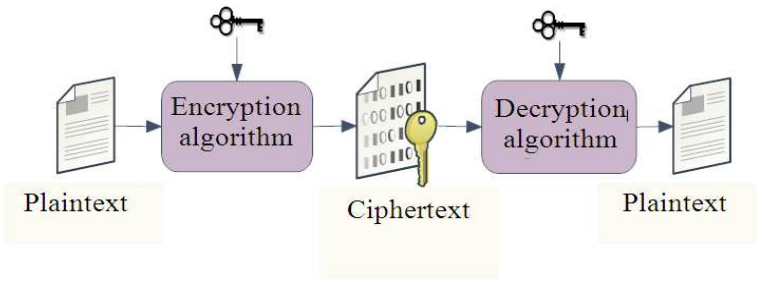

Fig. 1. Symmetric cryptography

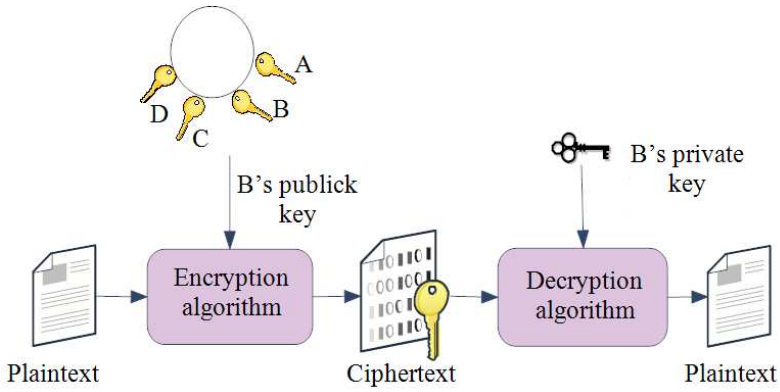

Fig. 2. Asymmetric cryptographty

Figure 1 shows the encryption and decryption of a given message. Plaintext, Ciphertext, encryption algorithm, decryption algorithm and secret key are considered to be the ingredients of symmetric cryptography.

Encryption: CT = E(K, PT)
Decryption: PT = D(CT, K)

Here, CT and PT are the ciphertext and plaintext respectively; K represents a secret key. This encryption method requires the key to be distributed to each other.

1.4. Asymmetric Cryptography

Here a pair of key namely public and private is used for encryption and decryption respectively. They are different key related to each other mathematically. Each user generates public and private keys. Public key is announced publicly whereas a private key is kept secretly. Each user also maintains a list of public keys of other users. Asymmetric cryptography need not to distribute key since all participants generate public and private keys locally. Plaintext, ciphertext, encryption algorithm, decryption algorithm, public key and private key are the ingredients of asymmetric cryptography. **Figure 2** explains the method of asymmetric cryptography.

The encryption and decryption of input message is carried as follows:

Encryption: CT = E(K_{Pw} PT)
Decryption: PT = D(CT, K_{pr})

where, K_{Pw} and K_{pr} are the public and private key of a user respectively. CT denotes the cipher text; plaintext is expressed as PT. E and D denote encryption and decryption algorithms. A profound example of the asymmetric algorithm is RSA. Elliptic Curve Cryptography, Diffie-Hellman and DSS are the applications where asymmetric cryptography can be applied.

RSA Algorithm

Rivest *et al*. (1978) invented RSA algorithm. RSA made use of exponentials. For establishing security in the internet, RSA is used. Its strength is its computational complexity. It is known for its security based on finding the prime factor of very large numbers.

1.5. Quantum Cryptography

Quantum Cryptography (QC) depends on the uncertainty principle of quantum with which it is impossible to for an eavesdropper to detect the data being transmitted without disturbing the transmission. This method is not based on mathematics instead it is developed on the base of physics. The changes made by the eavesdropper will anonymously introduce high error rate in the transmission between sender and receiver. It makes use of photons (light particles) to generate keys. Provably secure key distribution is achieved by using two channels between sender and receiver. Public and quantum channels are used to transmit encrypted data and key distribution respectively.

1.6. Linear Codes

A Linear Code C(n, k) over a field F is ventured in a vector subspace of F^n with dimension K.n which is called the length of the code C. The minimum distance (C) is found having the hamming distance d(x,y)which is being calculated by the formulae d: = min{d(x,y)|x,y ∈ C, x ≠ y}, Moreover (n, k, d) is judged as the parameter of C.

1.7. Proposed System

In order to provide security for messages and user personalized data, cryptography is used in wired and wireless communication. Mechanisms that suite wired network for affording security is not adaptable for wireless networks due to the mobile nature and link error properties of wireless networks. Therefore to provide security for ad hoc networks we proposed SKM technique. To implement SKM to nodes of ad hoc network we initially cluster the nodes. Nodes with high energy are chosen as Cluster Head (CH). One hop neighbour of CH (nodes within the range of CH) are grouped together to form cluster. CH of each cluster is responsible for generating pair of keys. Once keys are generated it is distributed to the nodes of the cluster. Distribution process is carried out by having mutual understanding between the cluster and CH. Following section elaborates our proposed technique.

1.8. Secure Key Management (SKM)

In our SKM, given data is converted into ASCII format. Then the following steps are carried out to securely transmit data from source to destination.

1.9. Key Generation

A Key is a piece of information, which acts as one of the inputs to an encryption algorithm. Resultantly the hard-hitting strategy lies in proving the security to an encryption system in protecting the key. The key generation is carried out using Hamming Codes at all the CH of an ad hoc network. Hamming codes are widely used in various fields such as telecommunication, computing and other applications. nxk dimension matrix is used for our approach to generate a matrix named Hamming Matrix which is denoted as G.

During transferring or storing data a set of error-correction codes called hamming codes are used in order to detect and correct the occurred error. An extension of error-correction code, hamming codes is devised with the concept of adding parity bits. Once these bits are added, data validation on be carried easily and can be checked on after reading and transmitting data. Thus the process of adding error correction code is an added advantage for error-correction code. It not only identifies a single bit error in the data unit, but also confirms its performance in locating the data unit. Suppose the leader node chooses this matrix for as [n, k, d] code.

For Instance consider a linear code of length 7, minimum distance 3 and dimension 4. It is called the Hamming (Bernstein *et al*., 2008c; Berger *et al*., 2009; Camtepe and Yener, 2004) code. Sharing like this is known as dual sharing. It is a general type of linear code constructed by using an algebraic curve X over a finite field F_q:

- Assume a matrix S having k X k dimensions. That matrix is termed as a private between the nodes. The private may be varying by interchanging this matrix
- Presume another matrix ‘P’ that has n X n dimensions
- Compute G’=G *S*P
- The computed matrix is said to be the Public Key matrix

From this we estimated the respective keys.

1.10. Encryption and Decryption Algorithm

Encryption and decryption process employs the method of McEliece algorithm:

- Plain text X id considered, which is embedded with the weight vector e
- The cipher text is computed to be
- Y = x*G + e
- Calculate approximately y_1=Y *P^{-1}
- This gives the encrypted text

The process of decryption is taken out through having the:

- The decryption process is carried out having y_1 by extracting the first four components of X_1 which is represented by X_0
- The analogous nodes will calculate $x = S^{-1} * X$
- Finally x gives the plain text.
- Thus the encryption and decryption process along with key generation is carried out having McElice Algorithm. Key distribution is given by the Dispense Key Approach

1.11. Dispense Key Approach

To exchange correspondence among a cluster of ad hoc network securely in a pair-wise fashion we proposed dispense key approach. Here, a pool of key pairs (public and private) K is maintained by an off-line trusted server. The public and private key of a key pair is mathematically related to each other. i^{th} key pair in the key pool is represented by $(k_{ipriv,}k_{ipub})$. To establish secure communication in ad hoc network, every member of each cluster is loaded with all public key of the group and assigned with a distinct private key. Let I_{PR} represents subset of private key of a user Alice and I_{PU} denotes the corresponding Alice's public key subset. If another user named Bob wants to sent a secret message to Alice, then Bob should know K_{PU}, where K_{IPR} is the anonymous destination (Here Alice is the destination). Bob encrypt the secret message with K_{PU} and send to Alice. The message can be opened only by Alice, who has the private key set K_{IPR}, but others do not. Let as assume an example having a cluster with 10 nodes. In Dispense Key, 5 distinct public-private key pairs are needed to build pair-wise secure communication channels among 10 nodes. They are:

$$\left(K_{1_{PR}}.K_{1_{PU}}\right),\left(K_{2_{PR}}.K_{2_{PU}}\right),\left(K_{3_{PR}}.K_{3_{PU}}\right),\left(K_{4_{PR}}.K_{4_{PU}}\right),\left(K_{5_{PR}}.K_{5_{PU}}\right)$$

In ad hoc network CH keeps 5 public keys and 2 private keys. Each node keeps a predetermined subset of private keys and no one will have private key for all the key pairs present in a subset, multiple copies of the private key can be held by different users. In the given circumstances, each private key has 4 copies.A message is encrypted by multiple public keys and it can only be read by a node that has the corresponding private keys.

If CH 1 encrypts a message m by public keys $K_{2_{PU}}$ and $K_{5_{PU}}$ as Enc (Enc (m, $K_{2_{PU}}$), $K_{5_{PU}}$), then only user 7 can decrypt it with private keys $K_{2_{PR}}$ and $K_{5_{PR}}$. In this way the pair wise keys are generated.

1.12. Experimental Results

Our proposed method is evaluated by deploying more nodes. The experimental setup is examined with AES, DES, RSA and McElice. Execution time, memory requirement and number of keys required for secure communication is analyzed for all the above-said algorithms. Following figures portrays that McElice works better than all other algorithms. It is also evident that our proposed method requires less execution time and memory requirement. In our experiment, the dimension of Hamming matrix is of the fixed form which is taken to be 7×4. This dimension in order to bring maintain the accuracy. Moreover, primary key is taken by interchanging of S matrix for those corresponding nodes.

1.13. Execution Time: Encryption

Our work is proposed method is analyzed with AES, DES, RSA. **Figure 3** shows that the execution time for McElice is low when comparing with others. The most widely used RSA algorithm requires a very large computation. This consumes time for encrypting the data. As ad hoc networks are resource based applying RSA to such a resource-based network is not advisable.

Since RSA will consume more battery of a mobile node so which becomes inefficient for ad hoc networks. Therefore, from resource-based network our proposed method's encryption algorithm works better than all other algorithms.

1.14. Execution Time: Decryption

Similar to encryption, execution time of decryption also affects node. **Figure 4** shows that encryption algorithm of our proposed method works well than all other algorithms taken for comparison.

Table 1, represents the summary of the key length, execution time for encryption and decryption of all the algorithms compared.

Table 1. Summary of algorithms

		Execution Time (seconds)	
Algorithm	Key length (bits)	Encryption	Decryption
DES	56	1.4	1.40
AES	256	1.6	1.49
RSA	1024	2.8	3.50
McElice	1024	1.2	1.30

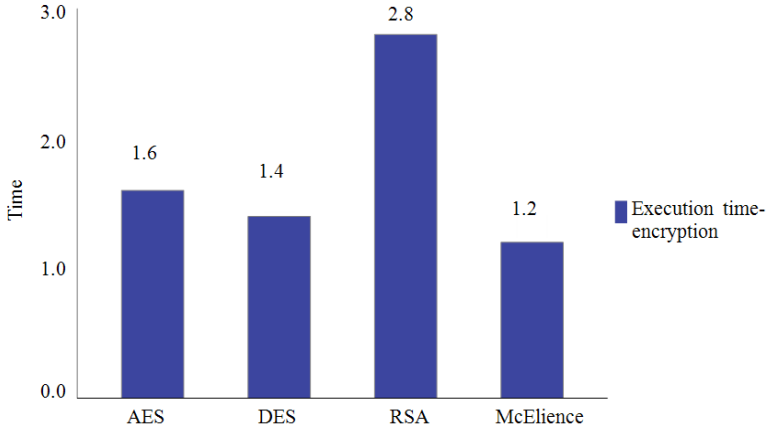

Fig. 3. Execution Time (Encryption) Comparison

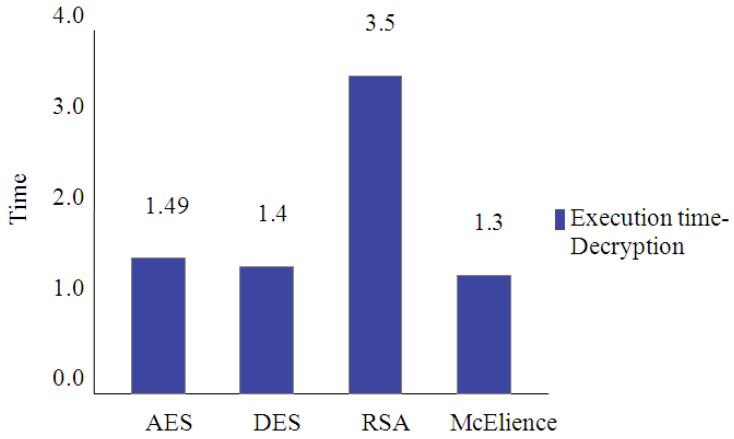

Fig. 4. Execution Time (Decryption) Comparison

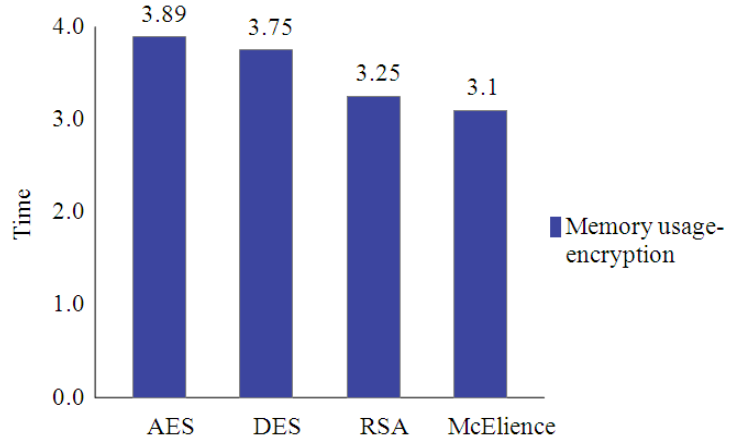

Fig. 5. Memory usage comparison-encryption

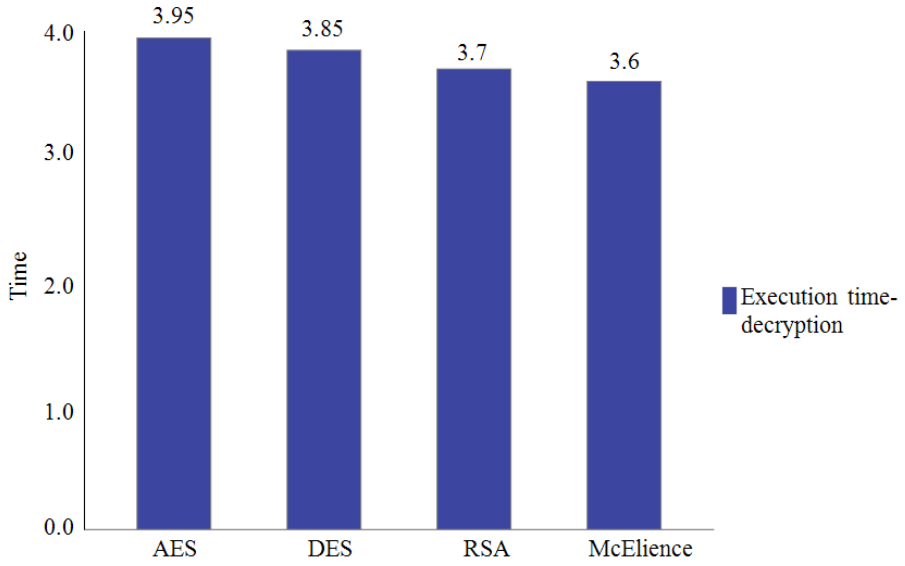

Fig. 6. Memory usage comparison-decryption

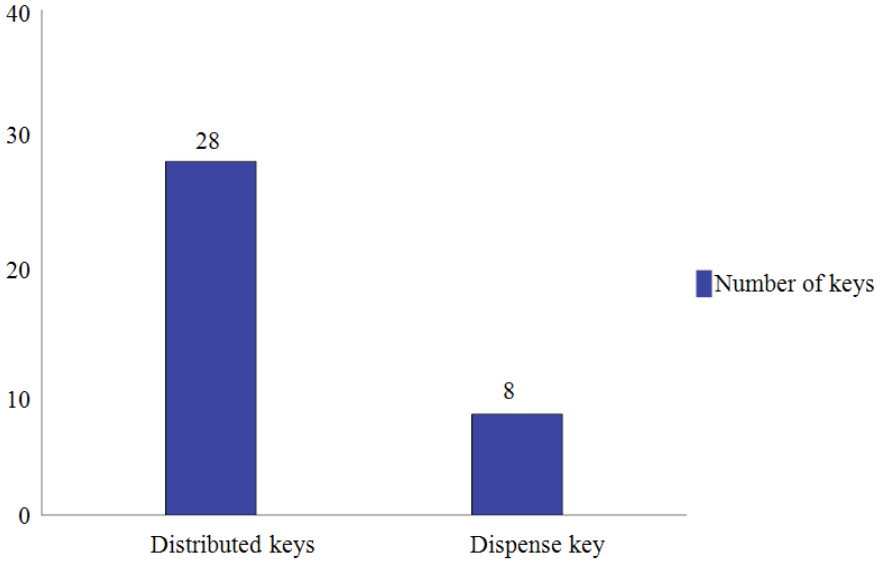

Fig. 7. Comparison between distributed and dispense key execution time: Encryption

1.15. Required Memory: Encryption and Decryption

Memory required for a node of an ad hoc network to carry out encryption and decryption using AES, DES, RSA and McEliece algorithms are explicitly shown in the **Fig. 5 and 6** respectively. If the memory requirement for secure communication increases, then processing of other user needed applications running speed on a node decreased. Therefore, it is needed for a resource network is that it should utilize memory in an effective way. It should not affect other processes running on the node.

Moreover, when proposing the Dispense Key approach the key management circumstances are very effective. For instance, we have considered some nodes, which are clustered initially. The leader node is

elected and the corresponding virtual group nodes are constituted by the nodes. It is observed that totally 14 key pairs are formed, but the used keys are only 8. In the previous approach which uses distributed scheme the neighboring nodes will create their individual keys in which the numbers of keys are very large with respect to the neighboring nodes say total key pairs are 14 out of that deployed keys are 28. This experimentation is portrayed in **Fig. 5**. Resultantly the numbers of keys are reduced in our proposed system. It is known that due to the portability the wireless device constitutes having limited bandwidth, memory and processing power. Consequently, the proposed approach SKM is adaptable for all the throughput constraints. These circumstances are depicted in **Fig. 7**.

2. CONCLUSION

Maximum of existing algorithms used for secure communication are not applicable to wireless scenarios. In order to adapt for wireless communications, we proposed SKM framework. In our SKM method, McEliece together with Dispense Key approach tends to be effective in both key generation and its management. As the key size is very large in McElice approach, it provides a secure authentication mechanism. Scalability of our framework outfits in terms of memory space and number of nodes. Experimental results in section 5 show that our method performs well than all existing algorithms such as AES, DES and RSA. The storage space for traditional self-contained public key management schemes is of O(n) order. With our proposed SKM framework in hand, we expect better scalability and still reducing time delay constraints than traditional broadcast authentication schemes. This will be investigated deeply in future work.

3. REFERENCES

Balasubramanian, S., H.W. Carter, A. Bogdanov, A. Rupp and J. Ding, 2008. Fast multivariate signature generation in hardware: The case of rainbow. Proceedings of the International Conference on Application-Specific Systems, Architectures and Processors, Jul. 2-4, IEEE Xplore Press, Leuven, pp: 25-30. DOI: 10.1109/ASAP.2008.4580149

Berger, T.P., P.L. Cayrel, P. Gaborit and A. Otmani, 2009. Reducing key length of the McEliece cryptosystem. Progress Cryptol., 5580: 77-97. DOI: 10.1007/978-3-642-02384-2_6

Bernstein, D.J., T. Lange and C. Peters, 2008a. Attacking and defending the McEliece cryptosystem. Post-Quantum Cryptography, 5299: 31-46.

Bernstein, D.J., T. Lange and C. Peters, 2008b. Attacking and defending the McEliece cryptosystem. University of Illinois at Chicago, USA.

Bernstein, D.J., T. Lange and C. Peters, 2008c. Attacking and defending the McEliece cryptosystem. Proceedings of the 2nd International Workshop on Post-Quantum Cryptography, Oct. 17-19, Springer Berlin Heidelberg, USA., pp: 31-46. DOI: 10.1007/978-3-540-88403-3_3

Camtepe, S.A. and B. Yener, 2004. Combinatorial design of key distribution mechanisms for wireless sensor networks. Proceedings of 9th European Symposium on Research in Computer Security, Sept. 13-15, Springer Berlin Heidelberg, Sophia Antipolis, France, pp: 293-308. DOI: 10.1007/978-3-540-30108-0_18

Chan, H., A. Perrig and D. Song, 2003. Random key predistribution schemes for sensor networks. Proceedings of the Symposium on Security and Privacy, May 11-14, IEEE Xplore Press, pp: 197-213. DOI: 10.1109/SECPRI.2003.1199337

Corlett, E. and G. Penn, 2010. An exact A* method for deciphering letter-substitution ciphers. Proceedings of the 48th Annual Meeting of the Association for Computational Linguistics, (CL '10), ACM Press, Stroudsburg, PA, USA., pp: 1040-1047.

Delgosha, F. and F. Fekri, 2006. Threshold key-establishment in distributed sensor networks using a multivariate scheme. Proceedings of the 25th IEEE International Conference on Computer Communications, (CCC' 06), IEEE Xplore Press, Barcelona, Spain, pp: 1-12. DOI: 10.1109/INFOCOM.2006.258

Du, W., J. Deng, Y.S. Han and P.K. Varshney, 2003. A pairwise key pre-distribution scheme for wireless sensor networks. Proceedings of the 10th ACM Conference on Computer and Communications Security, Oct. 27-30, Washington, DC, USA., pp: 42-51.

Engelbert, D., R. Overbeck and A. Schmidt, 2006. A summary of McEliece-type cryptosystems and their security. J. Mathem. Cryptol., 1: 151-199. DOI: 10.1515/JMC.2007.009

Kobara, K. and H. Imai, 2001. Semantically secure McEliece public-key cryptosystems-conversions for McEliece PKC. Int. Assoc. Cryptol. Res., 1992: 19-35. DOI: 10.1007/3-540-44586-2_2

Liu, D. and P. Ning, 2003. Establishing pairwise keys in distributed sensor networks. Proceedings of the 10th ACM Conference on Computer and Communications Security, Oct. 27-30, ACM Press, Washington, DC, USA., pp: 52-61. DOI: 10.1145/948109.948119

Rivest, R.L., A. Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Comm. ACM, 21: 120-126. DOI: 10.1145/359340.359342

Traynor, P., H. Choi, G. Cao, S. Zhu and T.L. Porta, 2006. Establishing pair-wise keys in heterogeneous sensor networks. Proceedings of the 25th IEEE International Conference on Computer Communications, (ICCC' 06), IEEE Xplore Press, Barcelona, Spain, pp: 1-12. DOI: 10.1109/INFOCOM.2006.260

Zhou, L. and Z.J. Haas, 1999. Securing ad hoc networks. IEEE Network Mag., 13: 24-30. DOI: 10.1109/65.806983