ISSN:0975-9646



# Review On: Privacy-Preserving in Wireless Networks

Vishal Mahajan[#1], Priyakanksha Mahajan[#2]
*A E Capital,Melbourne,Australia[#1]*
*Sr.System Engineer,Infosys Technologies,Melbourne Australia[#2]*

***Abstract: Wireless nodes are accumulated to form wireless networks. Such networks are mainly preferred by team on rescue mission, by military, and, many more. Privacy shows substantial role in communication in wireless applications. By two means the packet loss can be occur in wireless network, either by malicious packet drop or because of link error. The most preeminent task is to distinguish whether the packet loss is by virtue of link errors only, or by both malicious packet drop and link error. In this paper distinctive techniques such as Symmetric Cryptographic, Asymmetric Cryptographic, MD5, RSA, and ECC are deliberated that deals with the privacy preserving parameter of wireless network.***

***Keywords: malicious, symmetric, asymmetric, ECC, cryptography, RSA, MD5.***

## 1. INTRODUCTION

A Wireless Network that consists of sovereign devices named sensor nodes is a wireless sensor network. The sensor nodes normally have computational power low, can transmit limited data and there is power restriction. A network consisting of sensor nodes that can capture information arising out of an environment, perform data processing and transmission by the way of radio signals. Such wireless sensor networks can be established in different environmental area for measuring climatic, detecting the presence of smoke, and so forth, can be used in health area for measuring vital signs, temperature, in home automation where motion and image sensors are used and in many other fields wireless sensor networks are present and used increasingly in day to day life. Formerly, these networks have unsteady structure, and during the viable life of network, there is no monitoring station of sensor nodes in many cases. So a there must be a mechanism for self-configuration and adaptation in WSN in case of failure, addition or segregation of a sensor node.

In a wireless network, present nodes required to sustain the information related to their neighborhood because of various reasons, as for creating routes and for packet forwarding. For allowing proper operation of network, nodes required for distributing their identifiers, topology information and information related to location to other nodes. All the information then would be freely feasible to every node registered in a network, and even with a passive attacker which monitors the network's communication. Accordingly, it is apparent that single node can congregate much information about behavior of other users. The active attacks are more intricate in comparison with passive attacks. When a malicious node gets added in a network, then firstly it starts working in a coordinated manner for finding the route from source to destination. When malicious node gets added in the route followed for transmission, it stops forwarding the packets or starts dropping the packets that it received. Precisely, a dropping of packet can occur due to harsh conditions of channel as fading, interference and noise, known as link errors, or it can be because of the insider attacker of wireless network.

In wireless sensor network the Security requirements are akin to the traditional computer networks. For this reason the criterion like integrity, confidentiality, authenticity and availability must be considered for developing network's environment. All the solutions designed for security in traditional computer network cannot be directly implemented due to some limitations in wireless sensor network. Presently, aside from confidentiality, encryption also performs in area of integrity of verification can be depicted as:

***Confidentiality:*** It ensures that only the sender and receiver have the capability of understanding the message which is transmitted.

***Integrity*:** It is the capability of checking that if a message was modified at the time of transmission.

***Authentication:*** It is a medium for validating the identity of a respective communication.

It was accepted for a long time that the cryptography based on public key was not advisable for wireless sensor networks due to its requirement of high processing power, though studies of encryption algorithms on basis of curves was substantiated the practicability of the approach in wireless sensor network. Nearly all cryptographic algorithms are public. By keeping the algorithm public, it eradicates the creator from anxious cryptologist for decoding the system for publishing articles. Five years later if their exposure and no decoding were successful, it is assumed that the algorithm is solid. Reticence is the pivotal which has the operation of parameterizing the cryptographic function, it means only with the key a message can encrypted or decrypted. Another important factor is that the key have the capability of changing the output of the algorithm, so with every change of key, algorithm will engenders a new encrypted message. The size of key is critical aspect, as the longer the key is, more work has to be done by crypto analyst for trying to decrypt the message. In generic, sizes of keys are 64, 128 or 256 bits and can be lower or higher in accordance with the needs of security.

Currently, the RSA cryptographic algorithm is the extremely used algorithm amidst of the asymmetric algorithms, working from the difficulty of factoring large

prime numbers. This algorithm was standardized by NIST and is broadly used on the internet in transactions. Another algorithms created in 80s were ECC (Elliptic Curve Cryptography) and HECC (Hyperelliptic Curve Cryptography). These algorithms are based on the predicament of resolving the problem related to discrete logarithm on elliptic curves and hyperelliptic respectively. In spite of its intricacy the algorithm on the basis of elliptic and hyperelliptic curves have been widely studied in academicians. In recent days, an algorithm based on public key was proposed named as MQQ (Multivariate Quadratic Quasi Group). Experiments were performed in PC and FPGA podium showing that the MQQ algorithm is faster than RSA and ECC algorithms. The algorithms included in this study are asymmetric algorithms, though each algorithm works with a particular mode of encryption.

In wireless sensor networks, many studies evaluate the performance efficiency of cryptographic algorithms, though in performance analysis there is no standardization. For this reason the studies on performance appraisal of cryptographic algorithms are usually very peculiar in terms of platform, metrics, methodology and center of scrutiny. So, this paper construes an analytical study of algorithms as Symmetric, MD5, RSA, ECC, and MQQ (Multivariate Quadratic Quasi Group).

## 2. TECHNIQUES USED

***Symmetric Cryptography:***

In symmetric encryption (also known as secret key cryptography) a single key is used for both encryption and decryption of data. Till the 1976 year it was the only acknowledged technique used for encryption, although to be efficient and competent a secure channel is needed for communication where a cryptographic key can be altered.

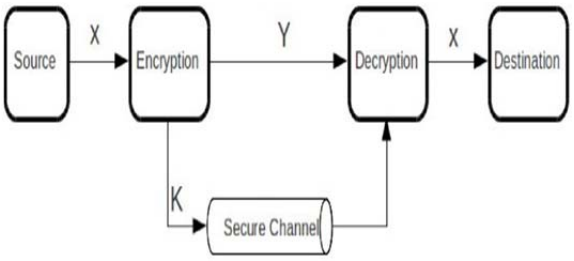


Fig 1: Symmetric Cryptography

Figure shown above delineates a communication taking place via symmetric encryption technique. The text is encrypted and X and Y become the message obtained through encryption algorithm and K is the secret key. Message Y is transmitted to the receiver, and receiver uses the K key for decrypting it, and converting it again into X. From figure 1 it is clear that the K key is carried by a secure channel. For its possession, a potential attacker can conveniently read the original text. AES (Advanced Encryption Standard) and DES (Data Encryption Standard) are two examples of symmetrical algorithms.

***Asymmetric cryptography***

Asymmetric cryptography (also known as public key cryptography) arises with a profound change of paradigms. Such public key algorithms are based on analytical functions, in lieu of substitution and permutation. In addition the one most essential thing is that cryptography based on public key is asymmetric, including the usage of two distinct keys, contrary to traditional symmetric encryption, that uses only a single key. The usage of two different keys has subtle consequences in the field of confidentiality, distribution of key and authentication. The preeminent differentiating feature of asymmetric encryption is that it permits the enactment of secure communication among individuals, beyond the prerequisite of previously shared single cryptographic key.

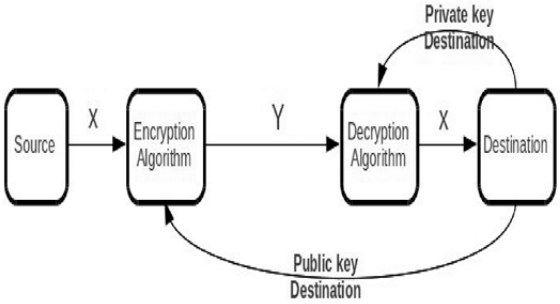


Fig 2: Asymmetric Cryptography

In this category of cryptographic algorithms two different keys are used for encryption and decryption naming a public key and a private key. In accordance with figure 2, public key is released by the receiver to the sender. Sender can encrypt the message by using the public key, although the private key of receiver is kept secret. This private key is used further for decryption.

***MD5 (Message-digest 5)***

The MD5 algorithm generates a 128-bit hash value. This harsh value formerly expressed in text format as 32 digit hexadecimal no. This algorithm is extensively used in field of cryptography and in diverse applications. MD5 algorithm is also commonly used for substantiating the data integrity. It is widely applicable in the software world where it provides some assertion that a transmitted file has arrived successfully without flawed.

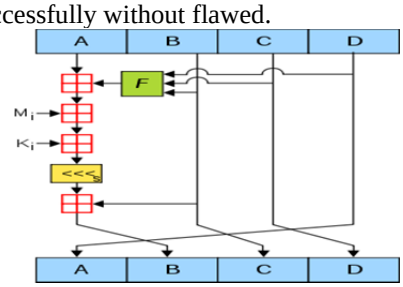


Fig 3: One MD5 operation.

Figure 3 shows one MD5 operation. There are 64 of similar operations in MD5 algorithm. A nonlinear function *F* is used in every round. A 32-bit block of input message is denoted by *Mi*. A 32-bit constant is denoted by *Ki*. For each operation this value is different. A left bit rotation is denoted by *s* and value of *s* changes for every operation. Additional modulo 232 is denoted by red color box in figure 3.

***RSA (Cryptosystem)***

The preeminent concept of those algorithms that are based on curves is to assemble a set of points of an elliptic curve for that the problem of discrete logarithm is intransigent. Cryptosystems are based on elliptic curves and is an intriguing technology as they attain same level of security systems just as RSA and accordingly engrossing less processor resources and memory. Such peculiar aspect makes cryptosystems excellent to use in smart cards and alternative environments where lineaments as time, energy and storage are restricted.

Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman are the person on whose initial letters of the surnames RSA was named. In 1977 RSA algorithm was firstly construed publicly. There are two phases in this algorithm which involves encryption and decryption and for both the phases different keys are used. In case of encryption, key is public and in decryption, key is secret. Public key is created by user and publishes it. This key is based on two large prime numbers and an ancillary value. The prime numbers used for creating public key is kept secret. This key can be used for encryption by anyone. Though if this key is colossal then someone with information of prime no. and ability can decrypt the message evidently.

In terms of encryption algorithm based on public key, RSA persists to lead the no. of exertions, though the no. of applications which use elliptic curves based algorithms is rising substantially thanks to the standardization achieved by NIST. The curve based algorithms are standardized in accordance to the FIPS 186-2, IEEE 1363-2000, ANSI X9.62, and ISO / IEC 15946-2. Encryption based on public key involves algorithms for key agreement, digital signatures and encryption.

***ECC (Elliptic Curve Cryptography) Algorithm***

In the mid-80 a method of cryptography was proposed based on elliptic curves named ECC algorithm. According to inventors of this algorithm, an elliptic curve is a plane curve delineated by the equation written below;

$$y^2 = x^3 + ax + b$$

This algorithm's efficiency is based on searching a discrete logarithm of an indiscriminate element which is part of an elliptic curve. To get a concept of relevance of the algorithms on the basis of elliptic curves with computational restraint contend that the competence and expertise of ECC algorithm with approximately key size of 160 bits. It is the same that is obtained by using RSA algorithm with key size of 1024 bit. Several features of this algorithm relied on elliptic curves, in addition to key management, digital signature and encryption. For sharing secret keys, key management algorithms are used and encryption algorithms facilitate a classified or secret communication. To authenticating a participant communication likewise validating the integrity of message, digital signature algorithms are used.

## 3. CONCLUSION

In this paper distinctive algorithms are construed that are used for authenticating sensor nodes and preserving privacy, especially for encryption and decryption of the data transmitted from source to destination. There are various algorithms that can be used for detecting malicious nodes and for encryption. Each algorithm has its own gains and loss. Symmetric and Asymmetric cryptography algorithms, RSA, MD5, and ECC algorithm are deliberated in this paper. In wireless sensor network, for enhanced efficiency an optimal algorithm should be considered.

## REFERENCES


[1] Tao Shu and Marwan Krunz "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks" in Wireless AdHoc Networks", June 2014.

[2] Mohammad A. Matin, "Wireless Sensor Network- Technology and Protocols" September 2012.

[3] Gustavo S. Quirino, Admilson R. L. Ribeiro and Edward David Moreno "Asymmetric Encryption in Wireless Sensor Networks" Universidade Federal de Sergipe, Brasil**.**

[4] Elliptic curve cryptography. More information on the site of the workshop on Elliptic Curve Cryptography which is in issue. Site: http://ecc2011.loria.fr/index.html

[5] B. Sun, Y. Guan, J. Chen and U. W. Pooch, Detecting black- hole attack in mobile ad hoc networks, In Proc. 5th European Personal Mobile Communications Conference, Glasgow, UK, April 2003.

[6] Amutha.S, Balasubramanian.K, "Secure Implementation of Routing Protocols for Wireless Ad hoc Networks" pp. 960-965, Feb 2013.

[7] Bobby Sharma Kakoty, S. M. Hazarika and N. Sarma "NAODV-Distributed Packet Dropping Attack Detection in MANETs" International Journal of Computer Applications (0975-8887), vol. 83- no. 11, 2013.

[8] Proano.A and Lazos.L "Packet-hiding methods for preventing selective jamming attacks" Dependable and Secure Computing., vol. 9, no. 1, pp. 101–114, Aug 2012.

[9] Shu.T, Krunz.M, and Liu.S, "Secure data collection in wireless sensor networks using randomized dispersive routes". Vol. 9, no. 7, pp. 941–954, Mar 2010

[10] Noble George and Sujitha M "Truthful detection of packet dropping attack in MANET" International Journal of Advanced Research in Computer and Communication Engineering, vol. 4 issue 7, 2015.

[11] M. Brown, D. Cheung, D. Hankerson, J. Hernandez, M. Kirkup, and A. Menezes, PGP in constrained wireless devices, In Proc. 9th USENIXSecurity Symposium, Denver, Colorado, August 2000.

[12] Dr. C. Kumar Charliepaul and K. Megala Devi "Secure routing and Attack detection in wireless AD HOC Network" International Journal on Engineering Technologies and Sciences, vol. 1 issue 6, 2014.

[13] Wang.C, Wang.Q, Ren.K, and Lou.W. "Privacy- preserving public auditing for data storage security in cloud computing", IEEE INFOCOM, Mar. 2010.