A New Secure Authenticated Key Agreement Scheme for Wireless (Mobile) Communication in an EHR System using Cryptography

Varun Shukla
PSIT, Kanpur
India

Atul Chaturvedi
PSIT, Kanpur
India

Neelam Srivastava
IET, Lucknow
India

ABSTRACT

In the modern era where the cut throat competition is going on, the rapid growth of the internet and the revolutionary shift of traditional communication methods by the internet services or group communication methods becomes paramount important. The other side of the coin says that there is a growing demand for security runs parallel. It is a well known fact that mobile phone or mobile devices are the best equipment for communication whether we talk about developing or developed countries. So keeping the security and authentication problem of mobile devices in wireless communication the authors present a secure authenticated key agreement based on commitment scheme for the Electronic Health Record (EHR) system where the security is extremely important and infringement in security issues can create various legal issues.

Keywords

Key Agreement, Authentication, Electronic Health Record (EHR), Security, Commitment, Man in the Middle Attack (MITM).

1. INTRODUCTION

It is important to know some basic fundamentals and terms of cryptography [18, 22]. The message is called as plaintext and denoted by M. The process of securing a message in such a way so that it is not readable for the external world is called encryption and usually denoted by $E(M)$. The encrypted message $C = E(M)$ is called cipher text. The process of turning cipher text back into plaintext, $M = D(C)$, is called decryption. Cryptography provides confidentiality but it is also used for:

Authentication: This security parameter is very important while communicating over an insecure channel because an active intruder will definitely be benefited because of the absence of authentication. Authentication also keeps the integrity of the message safe. In many environments, it is more important that communications are authenticated which means sender and receiver must trust each other’s identity so that communication is done between intended sender and receiver.

There are three methods we can use to authenticate someone:

- *Use something you have*: The example can be a key or a card. The disadvantage is that you can’t apply these methods every time because one can forget his or her card anywhere or one can steal that. They are not cost effective as well.
- *Use something you know*. All the calculations related to authentication fall into these categories. The advantage of using these calculations is that they can be efficient, and can be extended to higher calculations and also the number of entities using it. So when it comes to optimization of resources one always look forward for this approach.

Apart from these there are biometrics machines involving thumb impression and retina detection and can be utilized for authentication purpose. Authentication using these systems requires hardware and one to one interaction which is not possible in many cases and associated cost is also a problem. Authentication methods can be combined with several other things to strengthen the authentication security and level of protocol [4,7]. When somebody uses one of these methods, it is known as one-factor authentication. The usage of two techniques together is two-factor authentication. We explain this by an example. The cash flow process in an ATM machine utilizes two factor authentication. To authenticate, you present the ATM card (something you have) and enter PIN (something you know) then it calculates and grants the permission [19]. An enhancement to storing a password in plaintext on a system is to use a one-way hash function. Hash functions work on the concept of one way trapdoor and produce message digest values. A problem with passwords is that they can be stolen through observing a user's session. A stop-gap measure is to require users to change passwords frequently. Two-factor authentication generally involves using some form of calculation. Insecure channel is vulnerable to eavesdroppers and computation should be strong enough to maintain cryptographic goals [20]. One kind of challenge/response authentication problem works like this: In a client-server approach, a user is provided a challenge problem from the server with a prompt for the response. This challenge problem is entered into a challenge/response unit along with a PIN. This unit generates a response that is a function of the PIN, the challenge, and a key that is stored within the challenge/response unit. The response is copied back to the prompt from the server. The server maintains the user’s PIN and the key inside the challenge/response unit and can perform the same calculation and thus verify the response.

Key agreement: Key agreement as the name implies, is a process in which entities cooperate in order to establish a session key which is further used to encrypt the message. When it comes to peer to peer communication, key agreement becomes a necessity in order to transfer the data safely even in the presence of an intruder [1,2,3]. For communication security, symmetric cryptography, public key cryptography, or a hybrid system approach with involves both can be adopted.

To communicate using symmetric cryptography, both parties must agree on a same key (key agreement) named secret key. Sender and receiver utilize secret key for encryption and decryption. Key distribution in a secure manner is very important. In case of security compromisation, the identity of users can be impersonated which leads to failure of cryptographic goals [15, 21]. Public key cryptography has enough strength to solve this issue. Suppose *Alice* and *Bob* wish to communicate and they exchange their public keys for encryption. In that case, public keys should be kept in a reliable data base. RSA algorithm is an example of this [24], where M is the plain text, C is the encryption performed, D is decryption calculation, e and d are the public and private keys respectively, then we have

$$C = M^e mod\ n$$

And $$D = C^d mod\ n$$

Where n is the product of two large primes and which is the trapdoor. Generating an RSA key is an computationally expensive process compared to generating keys for symmetric algorithms, which basically involves picking a pseudo-random number. A common use of public key cryptography is to encrypt symmetric keys to solve the key distribution problem. It also enables an entity to pick a random key that will be valid for only one session. Suppose *Alice* and *Bob* wish to communicate. *Alice* sends *Bob* her public key. *Bob* then generates a random session key, encrypts it with *Alice's* public key, and sends it to *Alice*. *Alice* is now the only one who can decrypt the session key since only she has her private key, which is needed to decrypt the session key. After that, messages can be encrypted with the randomly generated session key. This type of cryptosystem, which is a combination of public key and symmetric algorithms, is known as a hybrid cryptosystem.

2. AUTHENTICATION AND KEY AGREEMENT FOR MOBILE DEVICES IN AN EHR SYSTEM

Communication networks have reached to an apex state where it becomes necessity in life. It allows us to access to online services at anytime, anywhere and by any device [14]. This brings out new services, that was previously only accessible via computers, now are available on mobile devices for e-commerce applications and various other services. These applications require mobile users to be authenticated in order to use the services [25, 27, 28]. Researchers have discussed [26] that people buy cell phones because they are the best communication devices. Respondents in research claim that cell phones are indispensable piece of technology in today's era. That means we always limit our mobile phone services and capabilities without proper authentication. So authentication is mandatory for using services such as e-commerce, e-business and other financial transaction services etc [8,16]. It is a current topic that user authentication and key agreement is very important for secure transactions of electronic health record implementation [8,9]. Electronic health record [EHR] is of no use if it is not secure and it has many users or parties (like patient, doctor, insurance agency) on the system so key agreement and authentication becomes very crucial for overall security.

An EHR is a real time record system which contains data related to patient health record like medical history, list of past operations/surgeries undergone, allergies, images related to x-ray scan, blood reports etc. In an EHR , various entities are the participants like patient, doctor, insurance agencies, test laboratories etc. This EHR system is very helpful in emergency situations when in urgency; a doctor can access patient's record over an EHR system and treat/operate him accordingly. There is no need of doing allergy test again. It can save time, money, efforts and in turn can save somebody's life. The EHR system is becoming very popular now a days, the countries like Canada is adopting this system. So in the upcoming years more countries tend to adopt this system. Security will be a very important issue in these kinds of systems because it contains sensitive information. Any unauthorized transfer of data may create serious problems. So security and authentication remain key aspects of developing EHR systems.

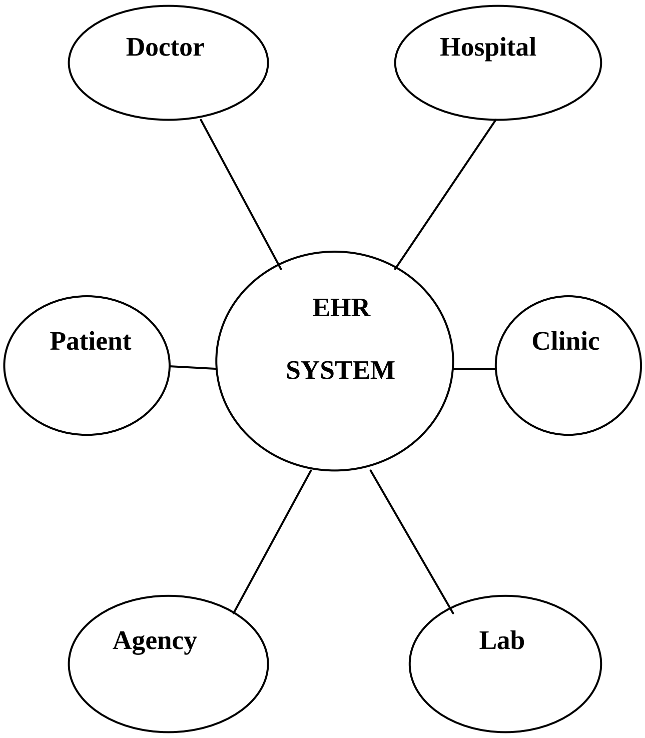

Figure-1: Showing possible (participating) entities in an EHR System

An unwanted or insecure communication in the EHR system may leads to serious problems or legal issues [11]. Consider a situation in which a doctor, in a communication process doesn't want to reveal the information of his patient because that may create problems in the insured amount. So when the doctor is communicating in this environment a common agreed key and authentication is mandatory. Now doctor or insurance agency want to communicate with patient and after that they want to submit their report to EHR system which can be a client server model. In that case authentic communication between doctor and patient is desired because it creates a device to device wireless communication system [29, 30] and a false information or altered data can create various legal issues or false health information may endanger somebody's life in the case of emergency or operation etc.

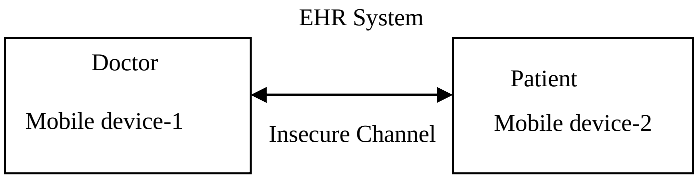

Figure -2: Showing communication between two entities of an EHR system over an insecure channel.

3. PROPOSED AUTHENTICATION AND KEY AGREEMENT PROTOCOL

(a) *Associated problems and assumptions*: We assume that two peers or two mobile devices are communicating for some health insurance/medicine data in an EHR system as participating devices [17]. So the desired communication can be done on a wireless channel. In the absence of a TTP (trusted third party) or any pre information regarding Alice and Bob (each other). It becomes mandatory to authenticate the sources then to agree on a shared secret key because in the absence of authentication an active intruder Eve can communicate with Alice and Bob and can raise legal issue on claim settlement/amount of balance premium etc [4,6,7].

Here Alice and Bob purposely want to authenticate each other for a very important conversation.

(b) *Strength of Attacker*: Our assumption regarding the attacker *Eve* is very clear. We assume that hacker can have full access to the wireless channel making it insecure. So he can alter or modify any message which deprives the cryptographic goal like integrity, confidentiality etc. The attacker can start conversation with any other user i.e. MITM is always possible and can be a very serious security concern [10].

(c) *Commitment scheme*: The term “commitment” is very important and specifically when it is used to design a cryptographic protocol [5]. Making a commitment directly means that a participant in a protocol is capable enough to select a value from a set or from a bit stream and commit to his choice so that he can not change his commitment later on [12]. This situation is analogues to a situation in that suppose there is a game between two players *Alice* and *Bob*. *Alice* wants to commit a bit α from the bit stream. Now *Alice* writes α on a paper, keeps that paper in a box and locks it with some mechanism say xoring of bits. Now *Alice* gives that box to *Bob*. Now here the strength of commitment lies; *Alice* can’t alter her choice but she has the freedom to reveal that choice at any time. A commitment scheme has two essential properties binding and hiding. In the above situation putting the paper in a box is binding and ability to reveal it anytime is hiding.

(d) *Protocol***:** The protocol presented, is a cocktail of Diffie- Hellman key agreement along with commitment scheme which contains binding and hiding properties. Let g denote a generator of a group Z_p^* where p is a large prime which is good enough for security.

Step-1: In the first step *Alice* and *Bob* both select a and b (randomly chosen elements in this group) as their private values and compute g^a and g^b . *Alice* and *Bob* have particular identity number $Alice_{ID}$ and Bob_{ID} which can be any number, name, code uniquely assigned to them [23].

Step-2: (Selecting random string and binding property): Here *Alice* and *Bob* randomly generate random string where the length of the string is kept limited to K-bit i.e.A_K and B_K .

Where $A_K \in \{0,1\}^K$

And $B_K \in \{0,1\}^K$

Here bit length K is very important parameter because it determines the scope of guessing i.e. the probability of making a brute-force in A_K and B_K.

Now *Alice* makes

$$Code_{Alice} \leftarrow Alice_{ID} \parallel g^a \parallel A_K$$

And similarly

$$Code_{Bob} \leftarrow Bob_{ID} \parallel g^b \parallel B_K$$

Now *Alice* develops a commitment scheme contains (b, r) where b is the binding lock and r is to unlock $Code_{Alice}$ in such a way

$$(b, r) \leftarrow Commitment(\, Code_{Alice})$$

Step-3: *Passing of parameters (Reveal Property)*: In this step *Alice* send b to *Bob* which is the commitment value. By getting b, *Bob* can’t reveal $Code_{Alice}$ but Alice can’t change her code now so that is binding. In reply *Bob* send $Code_{Bob}$ to Alice. On receiving $Code_{Bob}$, *Alice* send the reveal value r to *Bob* and *Bob* now can open $Code_{Alice}$.

An ideal commitment scheme is perfectly binding and hiding. The transmitter (*Alice*) has a private input ($A_K \in \{0,1\}^K$) and some common inputs. The commitment stage result in a joint output (b) which is the commitment on a particular value and a specific output (r) for the decommitment. So (b, r) is the pair. It is assumed that in an “honest execution”, the receiver (*Bob*) always accepts the incoming values from sender.

Step-4: *Authentication*: Now *Alice* and *Bob* both perform xoring of the randomly generated bit string A_K and B_K with the incoming value $Code_{Alice}$ and $Code_{Bob}$

$$U_{Alice} = A_K \oplus B_K$$

And similarly

$$U_{Bob} = B_K \oplus A_K$$

Since $U_{Alice} = U_{Bob}$ they both will agree on to exchange parameters for secret key sharing.

Step-5: *Passing of DH parameters and sharing a secret key*: Now *Alice* and *Bob* want to share a secret key for usage of symmetric cipher [13] but they are communicating over an insecure channel.

They have a groupZ_p^*, a large prime p with non zero integer $g\ modulo\ p$ where g is the generator.
Now *Alice* has selected a and *Bob* has selected b and kept them private. Here a and b are primitive roots. *Alice* will calculate $A = g^a\ (mod\ p)$ and send it to *Bob*. On the other side *Bob* will calculate $B = g^b\ (mod\ p)$ and does the same. Now *Alice* and *Bob* have each other's calculated values. Now *Alice* will calculate $A_{Alice} = B^a\ (mod\ p)$ and on the other side Bob will compute $B_{Bob} = A^b\ (mod\ p)$.

Now $A_{Alice} = B^a\ (mod\ p) \equiv (g^b)^a\ mod\ p \equiv g^{ab}\ mod\ p$

Also $B_{Bob} = A^b\ (mod\ p) \equiv (g^a)^b\ mod\ p \equiv g^{ab}\ mod\ p.$
So $A_{Alice} = B_{Bob} = S$ that is the shared secret key of the session for sharing important message in EHR system.

For better understanding we illustrate the above scenario by an example.
Let $p = 941, g = 627\ and\ a = 347\ , b = 781$ .So $A = 627^{347} mod\ 941 = 390$
and $B = 627^{781} mod\ 941 = 691$. So the pass values are $A = 390$ and $B = 691$.
Now $A_{Alice} = 691^{347}\ mod\ 941 = 470$ and $B_{Bob} = 390^{781}\ mod\ 941 = 470$ which is the shared secret key S.

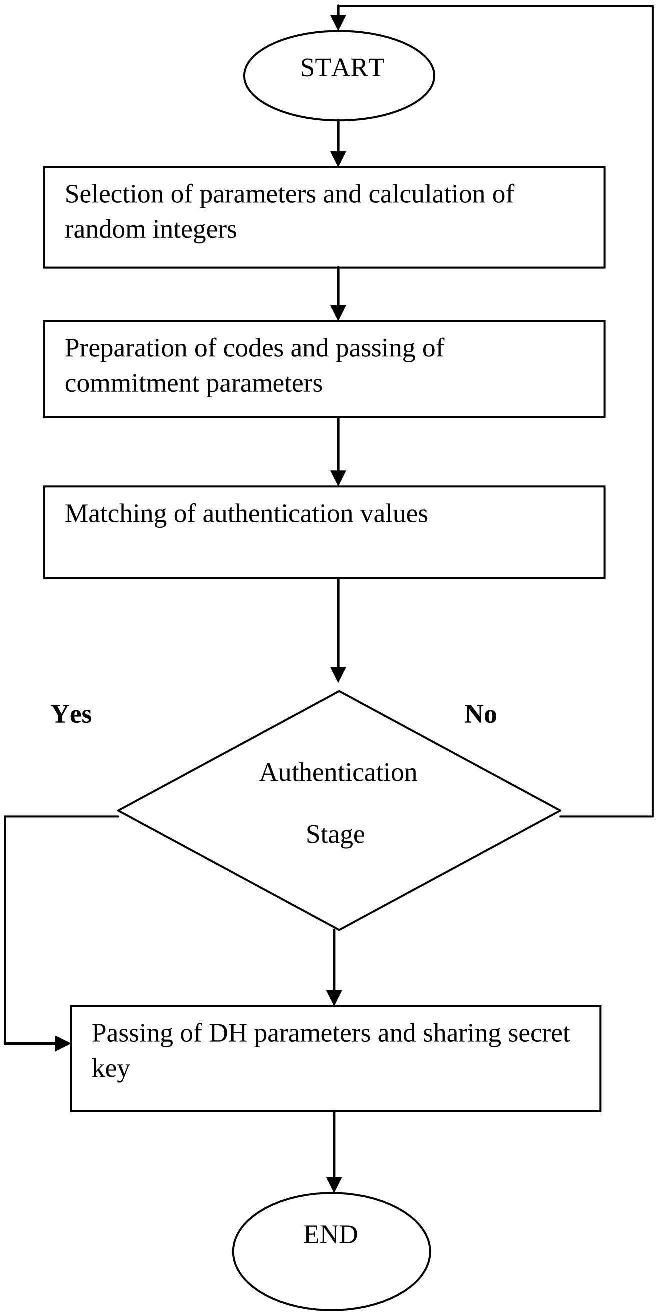
START
Selection of parameters and calculation of random integers
Preparation of codes and passing of commitment parameters
Matching of authentication values
Yes
No
Authentication Stage
Passing of DH parameters and sharing secret key
END

Figure-3: Showing the flowchart of above protocol

4. SECURITY ANALYSIS

(a) *Collision Free*: The commitment scheme (b, r) we are using is an ideal commitment scheme and that is our basic assumption. It means that the commitment value b is unique for $Code_{Alice}$ in such a way so that $b_{Eve} = b$ is never possible until $Code_{Alice}$ is not known. The same security assumption we have for r also.

(b) *Avoidance of MITM*: This is the very unique feature of our proposed protocol. If a hacker has full command over the wireless channel then also he would not be in the commanding position because of the nature binding/hiding property.

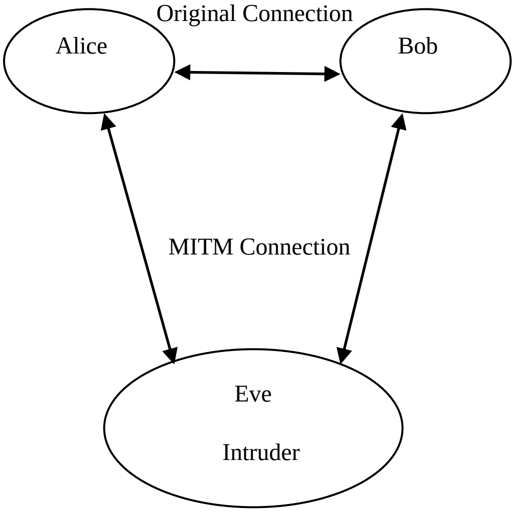

Figure 4: Illustrating the presence of intruder Eve in EHR system

Suppose *Eve* take the responsibility of protocol initialization as an intruder with *Bob* and pretends to be *Alice*. *Eve* will send his commitment value b_{Eve} to *Bob* which is the commitment of calculating the random string i.e.E_K where $E_K \in \{0,1\}^K$ and $Code_{Eve} \leftarrow Eve_{ID} \parallel g^E \parallel E_K$ and send it to *Bob*. *Bob* will send his code i.e $Code_{Bob}$ to *Eve*. Now *Eve* modify the incoming message from *Bob* and send it to *Alice*. In reply of that *Alice* will send (b, r) pair in which b is the commitment value which reveals no information about $Code_{Alice}$ but committed to a particular value only. So apart from all hacking effort, when it comes to the authentication stage of a protocol which is nothing but the calculation of U_{Alice} and U_{Bob}; the two bit streams will not match. As a result *Alice* and *Bob* will not communicate further and will not exchange their Diffie-Hellman parameters and that will save their computational overhead, time and all the hacking efforts of *Eve* will go in vain.

(c) *Probability of successful intruder attack*: The single chance of *Eve's* success is when *Alice* and *Eve* both generate a same random string (say *K* bits each). So the probability of success will be

$$P_{Eve\ (success\ )} = 2^{-K}$$

If we select $K = 20$ bits then $P_{Eve\ (success\ )} = 2^{-20}$ and that is equall to $9.53 * 10^{-7}$. Since $P_{Eve\ (success\ )}$ is negligible for 20 bit size than there is no question of discussing it and even bigger bit size will enhance the security level that in turn reduces the probability of success of *Eve*.

5. CONCLUSION AND FUTURE SCOPE

In the above discussion, the authors have developed a strong authentication key agreement protocol which is based on commitment scheme and in case of authentication failure it saves computational resources. This idea can further be implemented on group key agreement protocol where the various entities in an EHR system use (b, r) pairs for authentication which makes it very useful for wireless mobile communication. Another interesting future scope lies in the fact that only twenty bits random string creates very low probability of occurrence of brute force that means the protocol can be implemented on modern mobile devices with ease irrespective of the fact that they are transferring important EHR information with each other over an insecure channel where the intruder has full command to modify or alter the data.

6. REFERENCES

[1] Y. Amir, Y.Kim & C. Nita-Rotaru, " Secure communication using contributory key agreement", IEEE Transactions on Parallel and Distributed systems, pp. 468-480, 2009.

[2] A. Asadi and V. Mancuso, "WiFi Direct and LTE D2D in action," Wireless Days (WD), 2013.

[3] A. Asadi and V. Mancuso, "Energy efficient opportunistic uplink packet forwarding in hybrid wireless networks," in Proceedings of the fourth international conference on future energy systems, ACM pp. 261-262, 2013.

[4] D. Balfanz, D.K. Smetters, P. Stewart, and H.C. Wong, "Talking to strangers: authentication in Ad-Hoc wireless networks," in Proc. Network and Distributed System Security Symposium Conference, 2002.

[5] M. Bellare and and O. Goldreich: On Defining Proofs of Knowledge, Proceedings

[6] of Crypto '92, Springer Verlag LNCS, vol. 740, pp. 390–420.A. Boukerche, "An Efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc network", *IEEE Computer Communications*, Vol. 28, Iss. 10, 2005, pp. 1193-1203.

[7] J.Brandt, I.Damga°ard, P.Landrock and T.Pedersen: Zero-Knowledge Authentication

[8] Scheme with Secret Key Exchange, J.Cryptology, vol 11(1998), 147-160.A. E. E. Bresson, O. Chevassut, and D. Pointcheval(2003). Mutual authentication and group key agreement for low-power mobile devices. In Proceedings of MWCN 2003, pages 59–62. World Scientific Publishing.

[9] M. Cagalj, S. Capkun, and J.P. Hubaux, "Key agreement in peer-to-peer wireless networks," in Proc. IEEE (Special Issue on Cryptography and Security), 2006.

[10] A.Chaturvedi, N.Srivastava, V.Shukla, " A secure wireless communication protocol using Diffie-Hellman key exchange, International Journal of Computer Applications,Volume 126, number-5, September-2015.

[11] B. Dahill et al., "A Secure Routing Protocol for Ad Hoc Networks", IEEE ICNP, 2002.

[12] I. Damgard, B. Pfitzmann and T.Pedersen: Statsitical Secrecy and Multi- Bit Commitments, IEEE Trans.Info.Theory, vol.44 (1998), 1143-1151.

[13] W. Diffie, , M. Hellman (1976). New directions in cryptography. IEEE Trans. Inform. Theory, IT 22, No. 6, pp. 644-654.

[14] K. Doppler, M. Rinne, C. Wijting, C.B. Ribeiro, and K. Hugl, "Device -to- device communication as an underlay to LTE-advanced networks," IEEE Communications Magazine, vol. 47, no. 12, pp. 42-49, 2009.

[15] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA, October 27-31 2003, pp. 42–51.

[16] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA, November 18-22 2002, pp. 41–47.

[17] G. Fodor, E. Dahlman, G. Mildh, S. Parkvall, N. Reider, G. Miklos, and Z. Turanyi, "Design aspects of network assisted device-to-device communications," IEEE Communications Magazine, vol. 50, no. 3, pp. 170-177, 2012.

[18] B. A. Forouzan, "Cryptography and Network Security", Special Indian Edition, The McGraw- Hill companies, New Delhi, 2007.

[19] C. Gehrmann, C.J. Mitchell, and K. Nyberg, "Manual authentication for wireless devices," RSA Cryptobytes, vol. 7, No. 1, pp. 29-37, 2004.

[20] W. Mao, Modern Cryptography: Theory and Practice, Prentice Hall PTR, New Jersey, USA, 2004.

[21] A. Menezes, M. Qu, S. Vanstone (1995). Key Agreement and the need for authentication. PKS'95, Toronto, Canada.

[22] A. J. Menezes, P. C. V. Oorschot, & S. A. Vanstone, "Handbook of Applied Cryptography", 5th edn., CRC Press Inc., USA, 2001.

[23] RFC 2631, Diffie-Hellman Key Agreement Method, June 1999, Available at http://tools.ietf.org/html/rfc2631.

[24] R.L. Rivest, A. Shamir and L. Adleman, "A Method of obtaining Digital Signatures and Public Key Cryptosystems", Communication of the ACM, 21, 2(1978), pp 120-126.

[25] A.G. Saavedra and P. Serrano, "Device-to-device communications with WiFi Direct: overview and experimentation," IEEE Wireless Communications, vol. 20, no. 3, 2013.

[26] S.I.Siddiqui, S.Jabeen, M., Mumtaj, " Whether cell phone is a necessity or a luxurious item", Middle-East Journal of Scientific Research 19 (1): 61-65, 2014.

[27] J. Wang, Ch. Li, and J. Wu, "Physical layer security of D2D communications underlaying cellular networks," Applied Mechanics and Materials, vol. 441, pp. 951-954, 2014.

[28] C. Yu, O. Tirkkonen, K. Doppler, and C. Ribeiro, "Power optimization of device-to-device communication underlaying cellular communication," in Proc. IEEE ICC, pp. 1-5, 2009.

[29] C. Yu, K. Doppler, C.B. Ribeiro, and O. Tirkkonen, "Resource sharing optimization for device-to-device communication underlaying cellular networks," IEEE Trans. Wireless Commun., vol. 10, no. 8, pp. 2752-2763, 2011.

[30] D. Zhu, A.L. Swindlehurst, S.A. Fakoorian, W. Xu, and Ch. Zhao, "Device-to-device communications: the physical layer security advantage." in IEEE ICASSP, 2014