INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

SECURE AND USEFUL KEYLESS CRYPTOSYSTEM USING PUZZLE IN WIRELESS NETWORK

[1]Ms.S.NATHIYA M.E (CSE)*, [2]Mr.K.SATHISHKUMAR, M.E. +

[1]PG Scholar, PGP College of Engineering and Technology, Namakkal
nathicse885i@gmail.com
[2]Assistant Professor, PGP College of Engineering and Technology, Namakkal
Address: No. 42 A4/50, PVR Street, Mohanur Road, Namakkal – 637001., Tamilnadu, India
Mobile: 97 89 15 74 38

ABSTRACT

To secure our information with keyless cryptosystem is very complicated process in wireless network. It is sometimes shortened to InfoSec, is the practice of defending information from unauthorized access. There are two aspects of information security 1.IT (COMPUTER) security, 2.Information assurance. Wireless communications can be encrypted using protocols such as WPA/WPA2 or the older (and less secure) WEP. If a key that is weak or too short will produce weak encryption and also more no. of keys are used. To avoid more no. of key usage and time of encryption and decryption to use Time Lock Puzzle with puzzle establishment.
Time lock puzzle is used to hide the source address and lock the packet. In this, packet containing only plaintext of 8 bit or 64 bit information. Main Objective of puzzle schema to force recipient of a puzzle to execute predefined set of computation before extracting packets. First puzzle is send to the receiver, within the fraction of time packet will be send. Until solving the puzzle, the packet is stored in the buffer. If the puzzle is solved means, the source address is view to the receiver and also packet is extracted from the buffer. Then the information is received bit by bit because to reduce the data loss. Each user, timeslot will be set based on the puzzle. Through theoretical and experimental analysis, the TLP based trust model provides extra security with less key usage and also without encryption and decryption. TLP achieve High security with keyless cryptography with low computation and bandwidth in wireless network.

Index Terms: Timeslot, Puzzle Generation, Puzzle Extraction, Puzzle Establishment

I. INTRODUCTION

In wireless network physical security of the transferred data is not provided. Since the transmission environment is the air. An obligation for using cryptographic protocols. Mostly stream chippers are used to encrypt and decrypt the data transferred. In this network without cryptography, security is not possible.

This is fully based on information security in wireless system. A major challenge for large-scale systems is how to establish trust between different network without the benefit of trusted third parties or authorities. Usually the peers don't have any pre-existing relationship and may reside in different security domain such as cryptography techniques.

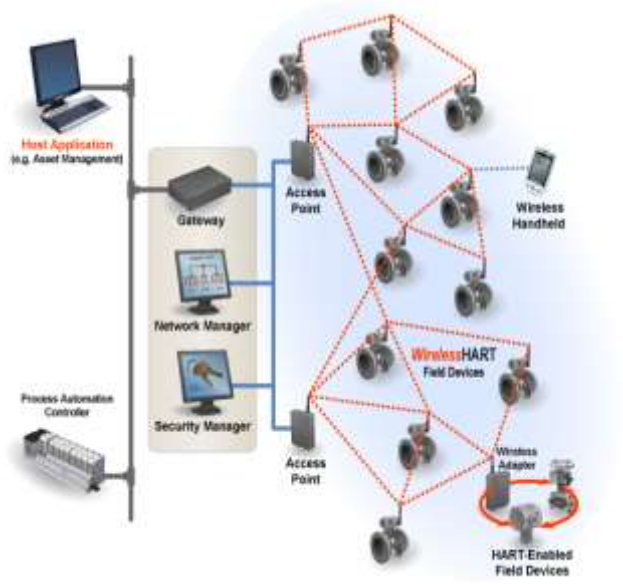
There are many reasons for wireless network, like mobility, simplicity, flexibility and accessibility. As the Internet's popularity grows, wireless network is becoming important. In addition, with the rapid development of network and communication technologies, new forms of such as wireless networks and mobile ad hoc networks—are quickly emerging.

Trust is an important issue in wireless network. Transactions in wireless network can cross domains and organizations, and not all domains can be trusted to the same level. Even within the same domain, users' trustworthiness can differ.

Trust management entails collecting the information necessary to establish a trust relationship and dynamically monitoring and adjusting the existing trust relationship. The various models for describing trust and trust establishment in distributed systems include public-key cryptography, the resurrecting duckling model, and the distributed trust model.

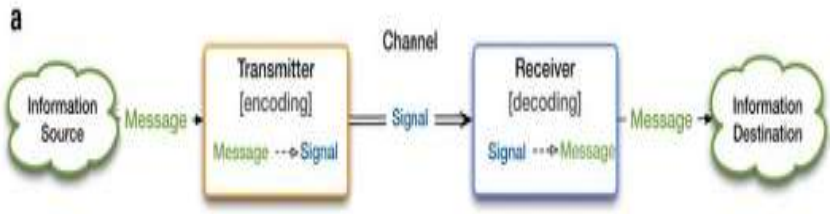
Crypto-less key establishment protocols based on anonymous channels have been introduced earlier. The main idea relies on establishing a secret key between two peers without using crypto functions but leveraging source indistinguishability of anonymous channels. Anonymous channels guarantee that an adversary cannot identify the actual signal source even if it is able to eavesdrop all the transmitted messages.

In such a scenario, two peers can exchange the bits of a secret message but it is not possible for an adversary to associate the current transmitted bit to the actual source. Such crypto-less algorithms are particularly useful in pairing of resource-constrained devices due to the fact that they do not rely on battery expensive computations. This paper presents COKE, a novel probabilistic crypto-less over-the-air key establishment protocol that guarantees secret key establishment in presence of a global eavesdropper without relying on cryptographic primitives. We present a detailed analysis about the adversarial capabilities to discover the exchanged secret key bits.



Commonly Gateway, Network manager, Security manager are used in wireless network for security purpose. Access point is used to accessing the nodes, which are participated in wireless network.

Normally encoding and decoding is used for security in wireless network. Mostly information's are send as a signal. The source side message is converted into signal and receiver side the signal is converted into message



SECURE key establishment between two parties can be addressed when public key infrastructure or an online trusted third party is available. These solutions cannot always be applied to resource constrained devices operating in pervasive environments because of both the lack of either a PKI or a TTP, and the high computation and bandwidth overhead required by asymmetric cryptography.

Secret key establishment between resource constrained devices realized without making use of crypto functions has been undertaken in mainly two different ways: extracting secret bits by observing the same physical phenomenon or exchanging secret bits anonymously without using crypto functions. We proposed a pairing algorithm based on exchanging packets with the source field chosen as a function of the secret bit to share; in this way, only the sender and the receiver know the actual value of the transmitted bit.

II. RELATED WORKS:

Wireless Sensors Network (WSN) security is a major concern and many new protocols are being designed. Most of these protocols rely on cryptography. To perform the keyless cryptosystem to use puzzles. In this, Time lock Puzzles is going to use and also puzzle establishment technique also used. This technique is fully based on condition and also time. Time management is very important one in information sharing of wireless network. Because this wireless network take our information as a signal.

[1] Coke is used for keyless cryptosystem using source address hiding and bit complementing process. Source address is hided based on random number generator [3]. The packet containing only 8 bit of information's, from that one bit is extracted and complemented for information security. Those processes are sensed by accelerometer [12].

Robust uncorrelated bit extraction methodologies for wireless sensors[4] presents novel methodologies which allow robust secret key extraction from radio channel measurements which sure from real-world non-reciprocities and a priori unknown fading statistics. This methodologies have low computational complexity, automatically adapt to deference in transmitter and receiver hardware, fading distribution and temporal correlations of the fading signal to produce secret keys with uncorrelated bits. Moreover, the introduced method produces secret key bits at a higher rate than has previously been reported. We validate the method using extensive measurements between TelosB wireless sensors.

Accelerometer [12] defines if two peers are carried by the same Person; this is center of the source and receiver. Receiver gets information's about bit complementing and source address but sender gets only on packet and bit complement. In this security is not occurs for remaining bits present in packet and also accelerometer.

Cryptographic Pseudo-Random Number Generator (CPRNG) is used to select the puzzles randomly [3]. Our generator uses the received bit errors as one of the sources of randomness. We show that transmission bit errors on a wireless sensor network are a very good source of randomness.

On the effectiveness of secret key extraction from wireless signal strength in real environments[5] evaluate the effectiveness of secret key extraction, for private communication between two wireless devices, from the received signal strength (RSS) variations on the wireless channel between the two devices. We use real world measurements of RSS in a variety of environments and settings.

Our experimental results show that (i) in certain environments, due to lack of variations in the wireless channel, the extracted bits have very low entropy making these bits unsuitable for a secret key, (ii) an adversary can cause predictable key generation in these static environments, and (iii) in dynamic scenarios where the two devices are mobile, and/or where there is a significant movement in the environment, high entropy bits are obtained fairly quickly.

Building on the strengths of existing secret key extraction approaches, we develop an environment adaptive secret key generation scheme that uses an adaptive lossy quantizer in conjunction with Cascade-based information reconciliation and privacy amplification. Our measurements show that our scheme, in comparison to the existing ones that we evaluate, performs the best in terms of generating high entropy bits at a high bit rate. The secret key bit streams generated by our scheme also pass the randomness tests of the NIST.

Random number generation:

Generation of random numbers is performed by using the block cipher in counter mode. One block operation is required for each 64 random bits generation. This means that the energy consumption is Proportional to the number of consumed random bits. Because this step is about 15.5 times slower than with a simple random number generator such as TinyOS's LFSR, it should be used with care when timing sensitive operations such as interrupts handlers or network drivers.

However, some precalculation of random numbers may be possible if some memory pool is available for buffering. This would ensure fast access to good quality random numbers. If ever the amount of random numbers requested is too high and it would be energy prohibitive to use TinyRNG, or the precomputed random numbers pool is empty, fast access to random numbers can be provided by the LFSR initialized with a seed from the output of TinyRNG.

On the energy cost of authenticated key agreement in wireless network [6] is to reduce the amount of data to be exchanged, and also reduce the decryption time which can be done by using special cryptographic paradigms like identity based and self-certified cryptography. [11] Fuzzy extractors, in this learn about how to generate strong keys and also find noisy data.[2] Shake: Single hash key establishment for resource constrained devices is used for puzzles establishment concepts.

III. PROPOSED METHODOLOGY:

In wireless systems, peers often must interact with unknown or unfamiliar peers without the benefit of trusted third parties or authorities to mediate the interactions.

Information security analysts are information technology (IT) specialists who are accountable for safeguarding all data and communications that are stored and shared in network systems. In the financial industry, for example, information security analysts might continually upgrade firewalls that prohibit superfluous access to sensitive business data and might perform defenselessness tests to assess the effectiveness of security measures.

This paper discuss about how the security will take place without more no. of key usage and also without any cryptography technique. In this sender send only plaintext to the receiver.

For that purpose, in this going to implement TIME LOCK PUZZLES. There many types of puzzles like rule based puzzles, time lock puzzles, etc...Rule based puzzles are used for sending packets to the future but encryption is take place with AES algorithm. This is fully based on condition. In this difficult to maintain time slots manually. So implementing Time Lock Puzzles.

- A novel probabilistic crypto-less over-the-air key establishment protocol TIME LOCK PUZZLES is introduced, that guarantees secret key establishment.
- In this we are hiding the source address and also Puzzle can be send before sending of information.
- Puzzle like a PWD to carry that information both information and puzzle are send one by another within the fraction of time.
- Information's are sending parallel but we are receive only bit by bit of information.

Time Lock Puzzle:

The key is introduced to hiding the identity of the source and not the content of the packet, to hide this packet using time lock puzzles algorithm, puzzles that guarantees secret key establishment.

PUZZLE GENERATION:

PUZZLES are generated based on

2^ (2^T) (MOD N)

Where,

N-Product of Two large prime numbers,

T-successive squaring modulo n, n=2…, compute w (t), is generated based on factor of n.

PUZZLE SOLVING TECHNIQUES:

Note that the puzzle can be solved by performing t successive Squaring modulo n, beginning with the value 2. That is, set

W (0) = 2
W (i+1) = (W (i) ^2) (mod n) for i>0,

And compute W (t). There is no known way to perform this computation. More quickly without knowing the factorization of n.

T value calculation:

Big integer value (t) is calculated based on

- squaringsPerSecond
- secondsPerYear
- squaringsFirstYear(S)

=secondsPerYear.Multiply (squaringsPerSecond);

Years = 35;
t = "0";
s = squaringsFirstYear;
For (int i = 1999; i<=1998+years; i++)
t = t.add(s);
Apply Moore's Law to get number of squaring to do the next year
Growth = "12204"; at constant rate
if (i>2012) growth = "10750";
Up to 2034, at constant rate s=s.multiply (newBigInteger (growth)).divide (new Big Integer ("10000"));

N value calculation:

Now generate RSA parameters
Prime length = 1024;
Pseed = large random integer for prime p seed
Qseed = large random integer for prime q seed
n = p.multiply (q);

E.g.:
The problem is to compute 2^(2^t) (mod n) for specified values of t and n. Here n is the product of two large primes, and t is chosen to set the desired level of difficulty of the puzzle.

Here is a smaller example of the puzzle.

Suppose n = 11*23 = 253, and t = 10. Then we can compute:
2^ (2^1) = 2^2 = 4 (mod 253)
2^ (2^2) = 4^2 = 16 (mod 253)
2^ (2^3) = 16^2 = 3 (mod 253)
2^ (2^4) = 3^2 = 9 (mod 253)
2^ (2^5) = 9^2 = 81 (mod 253)
2^ (2^6) = 81^2 = 236 (mod 253)
2^ (2^7) = 236^2 = 36 (mod 253)
2^ (2^8) = 36^2 = 31 (mod 253)
2^ (2^9) = 31^2 = 202 (mod 253)

w = 2^ (2^t) = 2^ (2^10)
= 202^2
= 71 (mod 253)

Thus, the "w" value computed for the puzzle is 71 (decimal), which is 47 (hex). If we have a "z" value for the puzzle of 13 (hex), then the "secret message" for the example is (47 xor 13) = 54 (hex). The secret Message should then be interpreted in ASCII at 8 bits per character.
To solve the puzzle, first compute w = 2^(2^t) (mod n). Then exclusive-or the result with z. (Right-justify the two strings first.)

The result is the secret message (8 bits per character), including information that will allow you to factor n. (The extra information is a seed value b, such that 5^b (mod 2^1024) is just below a prime factor of n.)

As part of the celebration of the 35th birthday of MIT's Laboratory for Computer Science, LCS Director Michael Dertouzos will present an "LCS Time Capsule of Innovations" to architect Frank Gehry. The Time Capsule will reside in the new building, designed by Gehry that will house LCS.

The time capsule will be unsealed on the earlier of 70 years from the inception of the Laboratory (on or about 2033), or upon

Solution of a cryptographic puzzle, described herein. This puzzle is designed to take approximately 35 years to solve. It uses the ideas described in the paper "Time-lock puzzles and timed-release Crypto" by myself, Adi Shamir, and David Wagner.

The value of t was chosen to take into consideration the growth in computational power due to "Moore's Law". Based on the SEMATECH National Technology Roadmap for Semiconductors (1997 edition), we can expect internal chip speeds to increase by a factor of approximately 13 overall up to 2012, when the clock rates reach about 10GHz.

After that improvements seem more difficult, but we estimate that another factor of five might be achievable by 2034. Thus, the overall rate of computation should go through approximately six doublings by 2034.

We estimate that the puzzle will require 35 years of continuous computation to solve, with the computer being replaced every year by the next fastest model available. Most of the work will really be done in the last few years, however. An interesting question is how to protect such a computation from errors.

If you have an error in year 3 that goes undetected, you may waste the next 32 years of computing. Adi Shamir has proposed a slick means of checking your computation as you go, as follows. Pick a small (50-bit) prime c, and perform the computation modulo cn rather than just modulo n. You can check the result modulo c whenever you like; this should be a extremely effective check on the computation modulo n as well.

In order to allow the LCS director in the year 2034 (or whenever) to verify a submitted solution, we have arranged things so that solving the puzzle also enables the

solver to factor the modulus n, as described below.

Of course, one way to break the puzzle is to factor the modulus n directly. But we have chosen a 2048-bit modulus, which is unlikely to be factored in the given time frame without a breakthrough in the art of factoring. Just as a failure of Moore's Law could make the puzzle harder than intended, a breakthrough in the art of factoring would make the puzzle easier than intended.

There many types of puzzles like rule based puzzles, time lock puzzles, etc...Rule based puzzles are used for sending packets to the future but encryption is take place with AES algorithm. This is fully based on condition. In this difficult to maintain time slots manually. So implementing Time Lock Puzzles.A novel probabilistic crypto-less over-the-air key establishment protocol TIME LOCK PUZZLES is introduced, that guarantees secret key establishment.

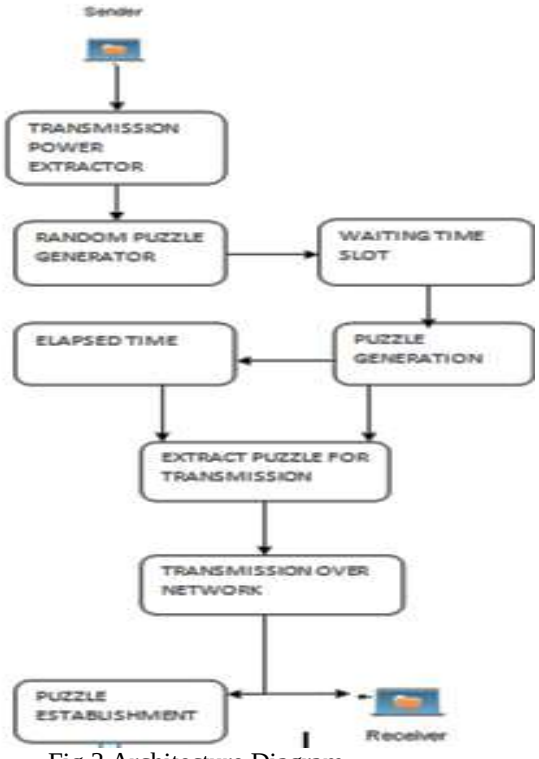


Fig 3.Architecture Diagram

IV. IMPLEMENTATION MECHANISM

The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly via intermediate nodes. Communication between the nodes is done by cryptographic mechanism. We present a novel probabilistic protocol (COKE) to allow two wireless communicating parties to commit over-the-air (OTA) on a shared secret, even in the presence of a globally eavesdropping adversary. The proposed solution leverages no crypto but just plaintext messages exchange.

Time Slots:

In this module, the bits are send by divided into different time slots and in each can perform one transmission. The users will try to send this bit to the other party via a single message based on the randomizing the source and the receiver address of the exchanged packets. Further, to make the slot contention fair, at the beginning of each slot each peer waits for a random time before trying to send its bit.

Hence, that bit will be stored by both the peers and will constitute the established one secret bit. If the sender would have been A, the bit would have been complemented and later stored. For the adversary it is difficult to guess how the exchanged bit will be stored by both the peers. Indeed, the value corresponding to the bit has been stored as transmitted (or complemented) uniquely depending on the ID of the sender.

Handling Packet Loss:

Wireless communication channels are prone to packet loss, and this may prevent secret establishment in COKE. For reducing the packet loss, each exchanged packet could carry a session ID and a sequence number. In particular, if one packet (bit) gets lost due to a wireless channel impairment, and lose their synchronization, and this will prevent the generation of the shared secret key. In order to make COKE robust to packet loss, we suggest to protecting the keys with an erasure code such as Reed-Solomon (RS).

Puzzle Generation:

Puzzle generation is the process of generating keys for Key establishment. This key is used for secure communication. We generate puzzle using Time-lock puzzle. A time-lock puzzle is a mechanism for sending messages "to the future". The sender publishes a puzzle, whose solution is the message to be sent, thus hiding it until enough time has elapsed for the puzzle to be solved. The puzzle is designed to foil attempts of a solver to exploit parallel or distributed computing to speed up the computation.

Puzzle Extraction:

Secret key establishment between resource constrained devices realized without making use of crypto functions has been undertaken in mainly two different ways: extracting secret bits by observing the same physical phenomenon or exchanging secret bits anonymously without using crypto functions. The communication peers are time-synchronized and time is divided into slots, and in each slot a device can perform (at most) one transmission. Further, to make the slot contention fair, at the beginning of each slot each peer waits for a random time before trying to send its bit. The shared bit will be stored by both the peers and will constitute the established one secret bit.

Minimize Transmission Power:

Our protocol introduces just a small transmission overhead when compared against other key-establishment solutions. Hence, our proposal is also an ideal candidate for those devices where computing capabilities are not a constraint, but energy consumption is, such as smart phones. The communicating peers are able to estimate the minimum transmission power which allows them to communicate each other's. Each node chooses a random power level to transmit the secret bit. The transmission power is chosen at random in the range, i.e., each node chooses a random transmission power between the minimum (guaranteeing the peer communication) and the maximum.

Puzzle Establishment:

Key establishment is process to establish a shared secret key available to two or more parties. Source creates the key, and securely transfers it to the destination. We assume all the communication packets are anonymzed, i.e., the source and the destination addresses does not reveal the real sender. For instance, a sender could randomly decide whether to use its own ID or the receiver ID to fill in the sender field. COKE needs just one hash computation for each shared secret key; such a computation introduces very low overhead.

V. CONCLUSION AND FUTUREWORK:

A crypto-less over-the-air key establishment algorithm that allows two peer to commit on a shared secret key without using preconstituted secrets or asymmetric crypto-functions. COKE requires exchanging a few one-bit messages between the parties for the shared secret to be built and requires only one hash computation for each generated secret key. Given its efficiency, it is particularly suited for resource constrained wireless devices, as well as for those scenarios where energy saving is at premium, Smartphone. A thorough analysis of the security of the proposed protocol is provided. This paper defined from a novel probabilistic crypto-less over-the-air key establishment protocol puzzle is introduced, and key is introduced to hiding the identity of the source and not the content of the packet, to hide this packet using time lock puzzles algorithm, puzzles that guarantees secret key establishment.

In the Future work

1. Give this security to high capacity packets like more than 64 bit.
2. Time slots can be set default based on puzzles.

REFERENCES:

1. Roberto Di Pietro and Gabriele Oligeri "COKE Crypto-Less Over-the-Air Key Establishment" IEEE transactions on information forensics and security, vol. 8, no. 1, january 2013.
2. P. Barsocchi, G. Oligeri, and C. Soriente, "Shake: Single hash key establishment for resource constrained devices," *Ad Hoc Networks*, vol.11, no. 1, pp. 288–297, Jan. 2012.
3. Goh W. L., Kong Z. H., Lan J., and Yeo K. S., "A random number generator for low power cryptographic application," in Proc. 2010 Int.SoC Design Conf. (ISOCC), Nov. 2010, pp. 328–331.
4. Croft J., Kasera S. K. and Patwari N., "Robust uncorrelated bit extraction methodologies for wireless sensors," in Proc. IPSN'10, 2010, pp.70–81, ACM.
5. Martinovic I., Schmitt J. B. and Wilhelm M., "Secret keys from entangled sensor motes: Implementation and analysis," in Proc. WiSec'10,2010, pp. 139–144, ACM.
6. Clark M., Jana S., Kasera S. K., Krishnamurthy S. V., Patwari N. and Premnath S. N., "On the effectiveness of secret key extraction from wireless signal strength in real environments," in Proc. MOBICOM 2009, 2009, pp. 321–332.
7. Gellersen H. and Mayrhofer R., "Password uncorrected bit extraction methodologies for wireless sensors," IEEE Trans. Mobile Comput., vol.8, no. 6, pp. 792–806, Jun. 2009.
8. Gosset F., Meulenaer G., and Pereira O., Standaert F.-X., "On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks," ser. WIMOB'08. Los Alamitos, CA: IEEE Computer Society,2008, pp. 580–585.
9. Azimi-Sadjadi B., Kiayias A., Mercado A., and Yener B., "Robust key generation from signal envelopes in wireless networks," in Proc.CCS'07, 2007, pp. 401–410, ACM.
10. Kirovski D., Sinclair M., and Wilson D., "The martini synch: Joint fuzzy hashing via error correction," in Security and Privacy in Ad-Hoc and Sensor Networks, ser. Lecture Notes inComputerScience.Berlin/Heidelberg: Springer, 2007, vol. 4572, pp. 16–30.
11. Castelluccia C. and Mutaf P., "Error correcting output codes vs. fuzzy support vector machines," in Proc. MobiSys'05,2005, pp. 51–64, ACM.
12. J. Lester, B. Hannaford, and G. Borriello, "Are you with me?—Using accelerometers to determine if two devices are carried by the same person," in *Book Series Lecture Notes in Computer Science*. Berlin/Heidelberg: Springer, 2004, vol. 3001/2004, pp. 33–50.

A Brief Author Biography

S.Nathiya **–** I obtained B.E(COMPUTER SCIENCE AND ENGINEERING) in PGP College of Engineering and Technology . Now pursuing M.E (COMPUTER SCIENCE AND ENGINEERING) in PGP College of Engineering and Technology under Anna University, Chennai. My research interests include Network Security.

K. Sathish Kumar **–** Completed M.E (COMPUTER SCIENCE AND ENGINEERING) from Anna University, Chennai. Working as Assistant Professor in PGP College of Engineering and Technology. My research interests include Networks.